2008-09

Net-centric information sharing supporting the 21st century maritime strategy

Green, Daniel M.

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NET-CENTRIC INFORMATION SHARING: SUPPORTING THE 21ST CENTURY MARITIME STRATEGY

by

Daniel M. Green

September 2008

Thesis Advisor:	John S. Osmundson
Second Reader:	Cary A. Simon

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Net-centric Information Sharing: Supporting the 21st Century Maritime Strategy		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Daniel M. Green			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This thesis analyzed Joint Vision 2020 and DoD Transformation technical concepts in the context of the "Cooperative Maritime Strategy for the 21st Century." It hypothesizes that Decision Superiority requires a renewed emphasis on the fundamentals of decision making. The thesis introduces the concept of Ignorance Management as a risk reduction concept to help focus decision makers, and the IT professionals who support them, on getting the "right information, to the right people, at the right time." The concept of Information Readiness Levels is explored as a means to help operational forces more objectively gage the ability of the information architecture to support decision making in the context of specific missions. One finding is that technical convergence has occurred and the promise of network-centric operations is becoming more fully realized as organizational and cultural evolution accelerates. Examples of organizational evolution are provided, including a survey of portfolio management and Communities of Interest policies. The thesis concludes with a case study of the Universal Core, an interagency information sharing initiative that exemplifies enterprise behavior, including political, technical and cultural progress in this area.

14. SUBJECT TERMS net-centric, UCore, decision superiority, SOA, XML, maritime strategy, ignorance management, right information, information sharing, communities of interest, portfolio management, information readiness levels, FORCEnet, change management, enterprise management, semantic web, web 2.0, Universal Core, navy data strategy,	**15. NUMBER OF PAGES** 97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NET-CENTRIC INFORMATION SHARING:
SUPPORTING THE 21st CENTURY MARITIME STRATEGY

Daniel M. Green
Civil Service, Department of the Navy
M.S., School of Engineering & Applied Sciences, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Daniel M. Green

Approved by: John S. Osmundson
Thesis Advisor

Cary A. Simon
Second Reader

David Olwell
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzed Joint Vision 2020 and DoD Transformation technical concepts in the context of the "Cooperative Maritime Strategy for the 21st Century." It hypothesizes that Decision Superiority requires a renewed emphasis on the fundamentals of decision making. The thesis introduces the concept of Ignorance Management as a risk reduction concept to help focus decision makers, and the IT professionals who support them, on getting the "right information, to the right people, at the right time." The concept of Information Readiness Levels is explored as a means to help operational forces more objectively gage the ability of the information architecture to support decision making in the context of specific missions. One finding is that technical convergence has occurred and the promise of network-centric operations is becoming more fully realized as organizational and cultural evolution accelerates. Examples of organizational evolution are provided, including a survey of portfolio management and Communities of Interest policies. The thesis concludes with a case study of the Universal Core, an interagency information sharing initiative that exemplifies enterprise behavior, including political, technical and cultural progress in this area.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

Acronym	Definition
ACTD	Advanced Concept Technology Demonstrations
ADNI	Assistant Director of National Intelligence
AMPS	Automated Metadata Population Service
ANSI	American National Standards Institute
ASD	Assitant Secretary of Defense
C4I	Command, Control, Communications, Computers, Intelligence
CBU	Controlled But Unclassified
CCTF	Common Core Task Force
CDM	Conceptual Data Model
CENTCOM	Central Command
CIO	Chief Information Officer
CM	Configuration Management
CNO	Chief of Naval Operations
COCOM	Combatant Command
COI	Community of Interest
COP	Common Operational Picture
CoT	Cursor on Target
CPM	Capability Portfolio Manager
CTISS	Common Terrorism Information Sharing Standards
DDMS	DoD Discovery Metadata Specification
DESC	Data Engineering Services Center
DHS	Department of Homeland Security
DIG	Description and Implementation Guide
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODAF	Department of Defense Architectural Framework
DOJ	Department of Justice
EBO	Effects Based Operations
EDE	Enterprise Data Environment
EDXL	Emergency Data eXchange Language
EO	Electro Optical
ESB	Enterprise Service Bus
ESC	Executive Steering Committee

ESC	Enterprise Service Bus
FEA	Federal Enterprise Architecture
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GIS	Geospacial Information System
IC	Intelligence Community
IC ISM	Intelligence Community Information Security Markings
IEPD	Information Exchange Package Documentation
IER	Information Exchange Requirement
IES	Information Exchange Specification
IRL	Information Readiness Level
IT	Information Technology
JCS	Joint Chiefs of Staff
JITC	Joint Interoperability Test Command
JV 2010	Joint Vision 2010
JV 2020	Joint Vision 2020
JWICS	Joint Worldwide Intelligence Communications System
LEISP	Law Enforcement Information Sharing Program
LEXS	Logical Entity eXchange Specifications
MDR	Meta Data Registry
MIEM	Maritime Information Exchange Model
NCES	Net-Centric Enterprise Service
NGO	Non-Governmental Organization
NIEM	National Information Exchange Model
NIPRNET	Non-Classified Internet Protocol Router Network
NORTHCOM	Northern Command
NSA	National Security Administration
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PEO	Program Executive Office
PII	Personally Indentifiable Information
PM ISE	Program Manager for the Information Sharing Environment
POAM	Plan of Actions and Milestones
PoR	Program of Record
PPBE	Planning, Programming, Budgeting and Execution
ROE	Rules of Engagement
ROI	Rules of Engagement

S&T	Science and Technology
SESGG	Senior Enterprise Services Governance Group
SIPRNET	Secret Internet Protocol Router Network
SIPRNET	Secure Internet Protocol Router Network
SKIP	Strategic Knowledge Information Portal
SKIWeb	Strategic Knowledge Integration Web
SLA	Service Level Agreement
SOA	Service Oriented Architecture
STRATCOM	Strategic Command
TADIL	Tactical Data Information Link
TCPED	Task, Collect, Process, Exploit, Disseminate
TPPU	Task, Post, Process, Use
UCORE	Universal Core
UCore	Universal Core
ULEX	Universal Lexical Exchange
USAF	United States Air Force
WWW	World Wide Web
XML	Extensible Markup Language
XSD	XML Schema Definition

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my wife and kids – Thanks.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THE NEW MARITIME STRATEGY

> The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn.
>
> Alvin Toffler

A. INTRODUCTION

A new maritime strategy was released in October 2007. Entitled "A Cooperative Strategy for 21st Century Sea Power," this document strikes a balance between traditional war fighting tasks and the historic maritime missions of deterring war, maintaining freedom of the seas, and developing partnerships for collective seaborne security (Allen, Conway and Roughead, 2007). The strategy acknowledges the unique role that forces afloat play in the execution of national power, regardless of whether that power is defined in political, economic or military terms. The document also represents an historic first in that it is co-signed by the Commandants of the Marine Corps, the Coast Guard and the Chief of Naval Operations.

Admiral Roughhead, the new CNO, highlighted examples of the practical execution of this strategy in an early December report to navy leadership called Rhumblines. On the 66th anniversary of the attack on Pearl Harbor, in addition to being engaged in combat related operations, the Navy and Marine Corps were concurrently assisting typhoon victims in Bangladesh, protecting international commerce from pirates off the Somali coast and engaging in maritime exercises with the navies of Gabon, Cameroon and the Ivory Coast (Roughead, 2007).

This strategy forces the Navy to reevaluate assumptions about DoDs' emerging net-centric capabilities in a context that stretches and potentially redefines the boundaries of the naval enterprise. These missions create data sharing opportunities and challenges that drive new requirements and test the agility of the Navy's enterprise architecture. This thesis describes the technical underpinnings of the net-centric data strategy, articulates the emerging role of Communities of Interest (COI) in the context of the new

maritime strategy, and provides recommendations for institutionalizing these concepts so that cyber power can more effectively support sea power.

B. BACKGROUND

Ten years ago, Albers, Garstka, and Stein examined the gentrification of the internet, the availability of low cost PCs and the emergence of the World Wide Web in the context of military mission areas. They postulated that these trends would create a unique operational environment and enable combat capabilities that were previously unachievable. The concept was dubbed "Network Centric Warfare" (Albers, Gartska and Stein, 1999). Encouraged by the initial commercial success of the dotcom industry, the Joint Chiefs of Staff incorporated this eCombat concept into their strategy and initiated a comprehensive re-architecting and modernization effort termed "transformation."

Chronologically bracketing the release of "Network Centric Warfare," Joint Vision 2010 and Joint Vision 2020 provided a strategic plan and end-state for creating a modernized force whose reach and lethality was improved through the access and use of information. Published in 1995 and 2000 respectively, these documents reflected both the uncertainties of the post-Cold War world and the nascent opportunities of the information age. Arguably the most compelling aspect of these two visions was that they appropriately estimated the time it would take DoD to transform. In the context of the two Joint Vision documents, transformation spans a full 25 years, from 1995 to 2020.

Looking back, even though we had good conceptual foresight, we can see that DoD and commercial industry were on the bleeding edge of many information age technologies at the turn of the 21st century. It has taken a decade of technological merger, standardization and experimentation to make the Net-Centric Warfare vision a feasible, cost-effective option. The convergence of packet switching, wide-band and wireless networking, Service Oriented Architectural patterns, XML-based data exchanges, and new data modeling standards; now provide the technical prerequisites for broad deployment that will contribute to the faster analytical cycles, better decision making and improved operational agility that was described in network centric theory.

C. DECISION MAKING

Capability is not achieved by technology convergence alone. It appears to be based on a non-linear technology adoption curve. Once technological maturity is reached, adoption can be stimulated by external environmental interventions (warfare), doctrinal and organizational changes and ultimately, human learning. Episodic or punctuated adjustments can radically improve capability, e.g., cruise missiles and UAVs. Adoption is also a function of resources. DoD may now be in a phase of modernization where it is more costly to stagnate and maintain legacy infrastructure than it is to invest in new technologies. Malcolm Gladwell defined a tipping point or "level at which the momentum for change becomes unstoppable" (Gladwell, 2000). Change gurus echo the same belief that transformation - once begun - takes on an unstoppable life of its own. This thesis addresses the ongoing transformation of data management in a net-centric environment. Technological tipping momentarily aside, one question is, how to move forward and lean into adoption.

D. SUPERIOR DECISIONS

One of the philosophical underpinnings of IT enabled communications centers around the term interoperability. IEEE defines interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" (IEEE 90, 1990). Colloquially, systems interoperability is understood to mean that systems can talk to each another. Early network centric theory proposed that more information contributed to better decision making, and that better decision making won wars. It spawned the concept of "Post Before Processing" and encouraged an unfiltered, high volume approach to decision support. The logic and allure of interoperability therefore, is that information sharing in and of itself, is a key enabler of mission accomplishment and battlefield victory. This is not necessarily so.

Information Superiority is defined by JV 2010 as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" (Shalikashvili, 1995). It indicated Information Superiority was one of the key tenets for operational success. However, the

subsequent Chairman of the Joint Chiefs of Staff, General Shelton, indicated in Joint Vision 2020 that information superiority is insufficient and that the true objective is decision superiority. "Decision superiority does not automatically result from information superiority. Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions" (Shelton, 2000).

This change in focus from information to decision superiority represented a tectonic shift that was intended to have a direct effect on the requirements levied on the Navy's enterprise architecture, investment strategy and procedures. An enterprise architecture tailored for decision making is much more sophisticated than that needed for mere information sharing. Information superiority is connectivity-centric. Decision superiority is knowledge-centric. Information superiority, connectivity-centric investment strategies stress radios, fiber, systems interoperability and networked nodes with requirements defined primarily in terms of bandwidth. A decision-superiority, knowledge-centric investment strategy stresses reasoning, analytics, decision criteria and business processes with requirements defined primarily in terms of data qualities (Kantner, 2001).

Connectivity and adequate bandwidth are generally accepted components needed for decision superiority strategy and execution. However, a preoccupation with bandwidth may have perpetuated sloppiness and inefficiency on the part of data producers, application developers and users. Requirements that cite lack of bandwidth, or the perceived need for ever increasing bandwidth, may contribute to a chronic condition of information overload and an unhealthy degree of data obesity. Investment decisions and enterprise level dialog that continually stress bandwidth may also limit needed discussion on efficiencies, cost savings and business process reengineering. DoD is finding it fiscally impossible to meet expectations for bandwidth that satisfy end-users who are conditioned by Google type searching and gigabit access to the World Wide Web (Powner, 2008). One conclusion is that most of the information shared over existing

bandwidth is never used for decision making. Because of information overload, most information produced, shared and stored is never used for any traceable purpose at all (Patterson, Roth, and Woods, 1999).

Superior decision making is a human function. Human factors engineer, Dr. Bob Smilie, indicates that human decision making can occur at a rate of about 70 bps (personal conversation March, 2008). Therefore, in its simplest form, the single overarching requirement of a decision superiority architecture is to present data to a human at a rate of 70 bps or less. This does not imply that decision superiority is not dependent on sharing potentially large amounts of information. It means that our infrastructure has to be groomed to support brainwidth limitation not bandwidth availability. It also means that organizationally we must focus on developing and managing predefined decision criteria which drive our data requirements. Superior decision making requires less information of higher quality thresholds than is being provided to decision makers today.

E. SUPERIOR DECISIONS AND THE DATA LIFE CYCLE

A generally acknowledged premise is that the Navy's ability to create an affordable information environment in which sustainable, superior decision making is the norm, will require more effective management of data across the entire data life cycle. This involves defining a user need, collecting, moving, storing, securing, sharing, analyzing, understanding and using data to make decisions, then archiving or disposing of the data after it no longer has adequate value. By focusing on the data needed for decision making, the entire IT infrastructure can be more effectively groomed to aggregate and filter the available information to meet decision quality thresholds. A consecutive series of superior decisions can lead to decision superiority, and when expanded to all applicable mission and business areas, it can also save precious resources. One view of the best way to manage bandwidth requirements is to reduce the amount of unnecessary information sharing, or noise, on the network. Similarly, a positive way to reduce the amount of data is not to collect it unless it can be traced to a decision requirement, including human (imperfect) generated requirements.

Since data incurs both initial and recurring costs at each phase of its data lifecycle, a shift in IT investment strategies from systems interoperability to a focus on the decision processes, and the data that supports those decision processes, is warranted. Capability based POM cycles have made some progress aligning systems to missions during budgetary tradeoff analysis. However, new architectural approaches such as Service Oriented Architecture (SOA) place less emphasis on systems and permit a loose coupling between data and the business logic used in the systems. In this design pattern, data becomes a semi-independent element within the enterprise architecture that requires additional management. In both complexity and duration, this is different from management of the systems that use the data. Additionally, since data is not tightly coupled to one system but can be used by many systems, it creates a need to deal with data at a management level above individual systems; at the enterprise-level. In this paradigm, mapping data to decisions cycles and defining the qualities of data needed to meet the threshold for decision making become the critical challenge. This is informally known as a requirement to get the "the right information, to the right person, at the right time" (Wennegren, 2007, p.1).

F. SUPERIOR DECISIONS AND DATA STRATEGY

Common knowledge again dictates that superior decision making requires management of data at the enterprise level, and management of data at the enterprise level requires a data strategy. The DoD Net-centric Data Strategy constitutes a data-level approach to interoperability. The purpose is to create an environment in which all users have an extremely high level of confidence in the information architecture. It is designed to further operationalize the notion of "right information, right person, right time." Rationally, this means that decision makers can define their needs, access data when it is available, share data that is accessed, and when it is shared, have confidence that it is fit for use. The Data Strategy articulates a vision with the implied requirement to ensure the quality of shared data is good enough to make decisions.

Subsequent chapters explore the concept of managing data as an enterprise asset throughout its lifecycle; from the identification of the information need until data

disposal. A generic data lifecycle approach provides a holistic methodology of viewing data and complements the emerging portfolio management construct for systems described in DoDD 8115.01, Information Technology Portfolio Management. Data lifecycle management also provides a process to define and align the new roles and responsibilities of data management that scale beyond traditional systems boundaries. Finally a data lifecycle approach permits various enterprise-level strategies to be implemented that optimize the physical and logical infrastructure and permitting organizations to achieve significant efficiencies and cost savings through specialization, collaboration and reuse.

G. DATA STRATEGY AND COMMUNITIES OF INTEREST

DoDD 8320.02, "Data-sharing in a Net-centric DoD," mandates compliance with the DoD Net-centric Data Strategy and provides a conceptual overview and high level considerations that bound the challenges and opportunities of data use in this technical paradigm. It requires data producers to make their data visible, accessible, understandable and trusted. These terms and the technical implications will be addressed in the following chapters of this paper. One of the most important aspects of DoD 8320.02 is that it defines a new managerial construct that crosses organizational, procedural and fiscal boundaries termed Communities of Interest (COI) as:

> A collaborative group of producers and users who must exchange information in pursuit of their shared goals, and who therefore must have a shared vocabulary for the information they exchange
>
> (Department of Defense [DoD] b, p. 2).

Organizational restructuring and procedural changes naturally lag technological evolution and COIs fill a gap created by the trend toward managing enterprise portfolios instead of stand alone programs. COIs are designed to exploit opportunities created by decoupling data from tightly integrated applications for enterprise level requirements. Unfortunately Communities of Interest reside in an area of temporary fiscal and organizational misalignment. The Planning Programming, Budgeting and Execution (PPBE), Acquisition and Requirements (JCIDS) processes are geared toward defining,

resourcing, building and sustaining systems, overseen by Program Managers and Program Executive Offices. As an Enterprise construct, COIs disrupt that paradigm. COIs place responsibility that was traditionally vested in the system builder and their data professionals, into the hands of the operator and a supporting data working group or Integrated Product Team.

The responsibilities of COIs are not trivial and are depicted in Figure 1 below. They imply a sophisticated level of understanding of data technologies as well as subject matter expertise in mission operations. Over the past 18 months, there has been a concerted push by the DoD Chief Information Officer to establish pilot implementations of Communities of Interest to establish lessons learned and best practices. The pilot implementations appear to be reducing risk and address a number of factors that are complicating implementation. A case study involving the COI concept and lessons learned will be described in greater detail in subsequent chapters.

• Identify elements from other COIs for reuse
• Define syntax and semantics for the COI
• Define Data integrity and quality control processes
• Identify data sources of record (based on business rules and appropriate agreements.)
• Define data stewards who manage the data asset
• Define data governance

Figure 1-1: Responsibilities of COIs (DoDb, 2004)

H. RESEARCH QUESTIONS

This research addresses several fundamental issues and concepts relating to the implementation of the net-centric data strategy within the Navy. The following chapters provide explanations and definitions for the following concepts and questions below:

- What is a practical approach to satisfying the requirements described as "right information, to the right people, at the right time"?
- What is a data life cycle?
- How is the data life cycle related to decision cycles?
- How do we define and manage data requirements at the Enterprise level?
- What is the role of data quality in a net-centric data sharing paradigm?
- What are the roles and responsibilities of Communities of Interest (COI)?
- How are Communities of Interest reflected in policy?
- How are COIs resourced?
- What organizational evolution is required to incorporate COIs into Navy's data management infrastructure and mission area portfolios?
- What is an example of Enterprise Management using COIs?
- What lessons learned can be derived from a COI case study?

I. BENEFIT OF THE THESIS

This research evaluates data sharing in a network centric environment as it relates to enterprise level systems architecting. It applies a system's engineering lifecycle model to enterprise data management and utilizes a case study analysis approach upon which the recommendations and findings are based. The objectives of this work are to enhance the body of knowledge on Communities of Interest and net-centric data sharing, analyze the extent of successful implementation of COIs, and recommend changes to policy and procedures that represent a practical, cost effective migration toward more rapid net-centric adoption.

J. SCOPE AND METHODOLOGY

A thorough review of the current literature on net-centric data sharing was performed and a best practices approach to enterprise data requirements management was

evaluated for its applicability to the maritime services. The Air Force, Army, Marine Corps implementation plans were evaluated for possible adoption by the Navy and Coast Guard. Maritime Domain Awareness, existing communities of interest, the Global Data Synchronization Network and the Universal Core initiative were used as case studies to derive lessons learned. Interviews were conducted with various Agency, Service and Joint practitioners including members on the staffs of the Air Force Chief Information Officer, Navy Chief Information Officer, Deputy Chief of Naval Operations for Communications (N6), Army Staff, Marine Corps Chief Information Officer, Assistant Secretary of the Navy for Acquisition, Department of Homeland Security Chief Information Officer, Defense Information and Systems Agency, Department of Justice Chief Technology Officer, and the Director of National Intelligence to validate assumptions. Interviews were also conducted with working members of various COIs and industry specialists to determine the capabilities and limitations of a COI approach.

K. SUMMARY

The network enabled military force envisioned in Joint Vision 2020 remains an overarching vision and goal, reflected in the National Defense Strategy released June 2008 (Gates, 2008). Additionally, the Chief of Naval Operation Strategic Studies Group XXVIII is tasked to explore one of the fundamental concepts of JV 2020, decision superiority, as an element of cyber power and determine how it can be more effectively implemented to support the new maritime strategy (Roughead, 2007). This year marks the halfway point in the modernization journey called Transformation, and technological convergence has finally reached the point where quantum improvements in capabilities may be realized. The maritime strategy, "A Cooperative Strategy for 21st Century Sea Power," creates information sharing opportunities and challenges that will flex and test the tenets of network centric warfare. A premise is that the Navy must challenge its assumptions regarding information and data sharing to focus less on volume, and more on the qualities of data that lead to superior decision making. New architectural paradigms decouple data and the systems that use the data, creating a need for managing data at the enterprise level, and new requirements for measuring the value of data throughout its

lifecycle. Cost effective implementation of decision superiority theory can be achieved by optimizing each phase of the data lifecycle and managing data through specific domains and organizations called Communities of Interest.

THIS PAGE INTENTIONALLY LEFT BLANK

II. INFORMATION SHARING IN SUPPORT OF DECISION SUPERIORITY

> Information provides the joint force a competitive advantage only when it is effectively translated into decisions.
>
> General Shelton (JV 2020, p. 13)

A. DATA DISCIPLINE

The former Chairman of the Joint Chiefs of Staff, General Henry Shelton, stated explicitly the dependency of the decision making process on information sharing in the context of military missions. This direct relationship with mission success requires an overarching, information sharing strategy managed through increasing levels of technical synchronization and human discipline.

On the Internet enabled, publicly accessible sites of the World Wide Web (WWW), requirements are driven by curiosity, marketing, the desire to be heard, the responsibility to inform and the mere fact that technology permits massive data sharing. In this era, information has come to be viewed as a freely available public good. Search engines like Google® index massive data volumes in tenths of seconds and add to the illusion that human knowledge is migrating to the web. Less than 10 years ago, the ability to simply expose data to a web-based browser was enough to create a global phenomenon called the .com economic boom. The Web created a technical veneer of credibility for the data available in that medium, although data were often of unknown or uncontrolled quality. The fascination with data exposure and sharing coincided with the development of DoD policies that changed the fundamentals of disciplined analysis and decision making. In 2000, Assistant Secretary of Defense (ASD) for Command, Control, Communications and Information (C3I), John Stenbit, directed all data producers to "post data before processing" in order to achieve a theoretical time advantage that could

hasten the decision cycle. Unfortunately, both the .com economic bubble and the decision theory that relied solely on data creation and exchange both proved unsustainable (Nordhaus, 2004 and Powner, 2008).

When the Web is used for business, data sharing requirements are driven by factors related to achieving premium profits, e.g., security, timeliness, accuracy, non-repudiation and the overall demand for high quality information. In this environment, efficiency – vice volume – appears to be paramount. Excess, low quality information contributes to clutter and noise that confuses the demand signal for commerce. It clogs communication arteries and increases transaction time, can become a legal liability in terms of displayed personal information, and adds directly to costs. At this point in history, the Navy, and DoD are caught in the middle of the two, sometimes competing approaches to Internet / WWW usage: the ability to share, and the desire to be productive.

The three primary military networks, Non-Classified Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communication System (JWICS), are constructed and dependent on internet standards and protocols, best practices and procedures developed from experience on the World Wide Web. Network Centric Warfare is a practical application of these technical protocols and practices as they apply to military missions and business processes. Policies like DoD Directive 8320.02, "Data Sharing in a Net-centric DoD," and Chairman of Joint Chiefs Instruction 6212.1D, "Interoperability and Supportability of Information, Technology and National Security Systems" direct DoD systems providers to migrate to Internet Protocol based communications, web-based applications and publish and subscribe information sharing paradigms. As of summer 2008, migration is proceeding slowly with Major Defense Acquisition Programs Network Enabled Command and Control, Network Centric Enterprise Services, and Distributed Common Ground Station just starting to deliver capability based on the adoption of foundational concepts such as web-services, Services Oriented Architecture (SOA) design patterns and Enterprise Service Bus technology.

B. DECISIONS AND DATA

Decision superiority is a condition in which humans derive consistently valid conclusions from the analysis of information and initiate actions that lead to mission accomplishment based on these conclusions (Wikipedia, 2008). From a human perspective, a decision is a choice made between alternatives. In a well run business or military operation, rational choices are based on decision criteria. Decision criteria are quality attributes that guide decision makers along various tradeoff arrangements. A decision point is that stage of a military mission, business process, or a crisis where alternatives exist and therefore choices must be made. A decision maker is the person who possesses the authority and responsibility to chose between alternatives that are consequential for mission or business success.

Although humans can make decisions from experience, gut feel or intuition, complexity and a fast changing environment may overload the lone decision maker. The system design challenge is to understand the decision making context, then to inject relevant and usable information throughout the process to assist decision makers. This concept is captured in the design heuristic, "right information, right person, and right time." The goal of information sharing is to tee up actionable alternatives from available data to improve decision making.

Data is defined as a set of facts that can be used to draw conclusions (Wikipedia, 2008). A fact is a statement or an assertion about something. A verified fact is considered truth (Wikipedia, 2008). In theory, decision superiority is enhanced by a computer's ability to manipulate large amounts of digital factual data, including those that represent true facts, sharing these true facts and aggregating them into alternatives. This may permit choices to be made faster, with more consistency and with more confidence. The relationship and value of a data sharing architecture used for decision making is a function of: (1) the ability to validate facts; and (2) the degree of linkage between facts and mission or business tasks. Figure 2-1 below depicts the concepts and actors involved in a notional human decision cycle.

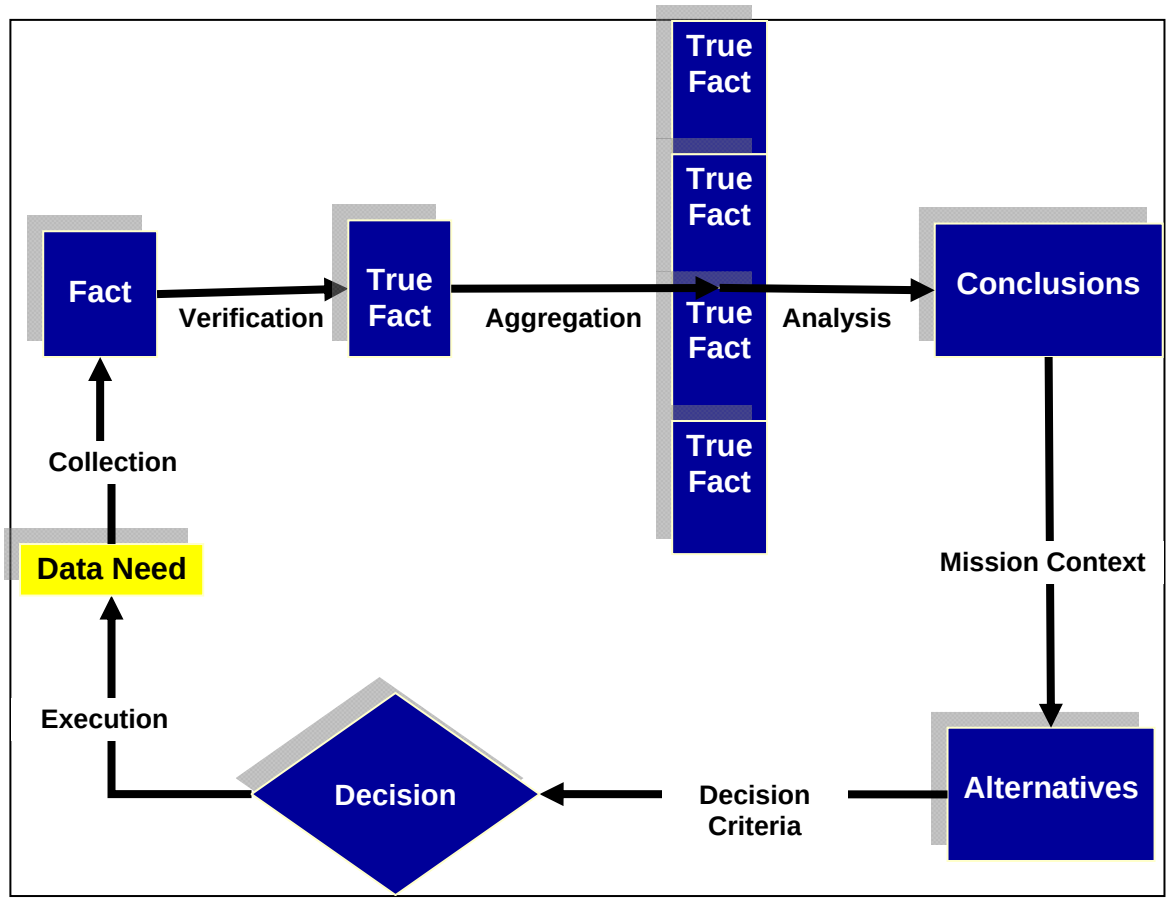


Figure 2-1: Notional Decision Cycle

In combat, decision superiority implies that a military commander's decision cycle can be executed faster than the time it takes for the enemy to react. The following scenario, based on real-world events is used to illustrate the basic relationships between decision superiority, information sharing and data quality.

C. DECISION SCENARIO

In January 1999, the USS Carl Vinson Battle Group was operating in the northern Arabian Gulf enforcing United Nations sanctions against Iraq. The previous month, President Clinton ordered a massive strike, known as Desert Fox, in response to Saddam Hussein's banishment of the UN weapon's inspection team. After Desert Fox, Saddam initiated a militarization of the Al Faw peninsula in southern Iraq in direct violation of UN brokered agreements to maintain the peninsula as a demilitarized zone after the Gulf

War. This violation included movement of CSSC-3 Seersucker surface-to-surface cruise missiles into the area. With a range of 25 nautical miles, the mobile Seersuckers could target the U.S. and coalition ships conducting United Nations Maritime Interception Operations in the most northern patrol areas of the Gulf. The movement of the missiles to Al Faw was declared a hostile act and Rules of Engagement were promulgated that permitted actions to be taken to eliminate the CSSC-3 from the peninsula. Since they were mobile, however, their exact location was unknown.

Data collection operations were initiated and tactical and national Intelligence, Surveillance and Reconnaissance (ISR) assets were tasked. Due to the nature of this particular target, the only sensor suite that would provide the data of high enough quality to trigger a decision was Electro-Optical or EO. EO sensors are essentially cameras (more formally known as apertures) that are mounted on aircraft and are imbedded payloads on satellites. An electro-optical aperture creates a data product known as an image. The image is interpreted by intelligence analysts with a variety of systems. In this case the data quality had to be enhanced by mensuration, i.e., electronically measuring the image to obtain the 3-dimensional geographic coordinates necessary for precision weapon engagement.

F-14 Tomcat aircraft equipped with new digital EO imagers called TARPS conducted independent, daily reconnaissance flights over the Al FAW. One day, due to intelligence cuing, an F-14 pilot and navigator were able to visually locate a suspected CSSC-3 transported erector launcher (TEL). The pilot maneuvered the aircraft and successfully captured images of the CSSC-3 with a missile loaded on the spell (TEL) rail. He made a radio voice report and returned to the carrier. Once within line of sight of the carrier, the image was transmitted to a TARPS receiver and processed by the imagery interpreter who extracted the coordinates and verified that this was a CSSC-3 TEL with missile. The Senior Intelligence Officer validated the finding of the imagery interpreter and reported his findings to the Admiral's staff. The image was also loaded to the NIPRNET and sent to the Admirals staff and back to Central Command (CENTCOM) headquarters via email.

The Admiral received a briefing from his principle staff assistants, the N2 (e.g., intelligence), the strike commander (aka CAG) and the lawyer (aka JAG) who provided their perspectives on the validity of the data, verified the ROE and offered alternatives for a strike. The Admiral weighed his options and made the decision to order the strike. The strike was conducted by an F-18A with a precision weapon. The pilot reported that visually the CSSC-3 appeared to be destroyed. The strike Commander launched another TARPS mission to collect a second image to collaborate Bomb Damage Assessment. An intelligence analyst verified the pilot's initial report through analysis of the new image and transmitted a report up the chain of command. The Admiral notified CENTCOM who notified SECDEF who informed the President.

In this scenario, the battle group commander had a clear need for information, and well-defined decision criteria keyed to previously approved Rules of Engagement. The commander was prepared to make the decision to strike the target when the information collected met the ROE conditions and quality threshold. In this entire scenario, there was one significant piece of data that triggered the decision cycle and allowed the Admiral to achieve decision superiority: the image. The image was a "fact" that could be validated as true. It provided visual evidence that the threat had been located and was used to generate machine readable coordinates that defined where the target was at a specific time.

No other piece of intelligence information or set of information elements would have met the quality criteria for the Admiral to make the decision in the context of his quality criteria and ROE. If that information had not been available or if it had not been shared, no action would have been taken. The players in this case, from the Admiral, his staff, the pilots and the analysts all understood the decision criteria. This allowed them to collectively filter out all other potential sources of data that, through their experience, use of Standard Operating Procedures and ROE, they knew would not be satisfactory. Although largely manual, this scenario contains all the elements of effective decision making and satisfied the two criteria for an effective data sharing architecture stated above: (1) support the ability to validate facts, and (2) link the data to mission or business tasks.

This decision superiority scenario was successful because of a high degree of discipline in both planning and execution. The intellectual capital of dozens of highly trained professionals was brought to bear on the problem, the data qualities and decision points were predefined and the validity of the information product (i.e., the image) was known. Due to the tremendously larger volumes of data available to support decision making today, the current challenge is to automate portions of the decision cycle by imbedding the data aggregation, filtering and quality assurance functions into the decision cycle so that the human staff can use computers and the network for more effective decision making.

D. DATA CENTRIC ANALYSIS: "YOU ARE A PHOTON"

During his 34 year tenure as the director of naval nuclear power, Admiral Hyman Rickover required that all nuclear power school students be able to trace a molecule of water through its many transformations from seawater, through the nuclear power plant and back to the sea. He rightly assumed that this would foster a complete understanding of the architectural relationships in what was essentially a physical link and node network. The following section is designed to foster an understanding of the process by showing how data is created, interpreted and sometimes transformed during a decision cycle. The combat scenario from the previous section will be used for the sake of continuity.

At the human level the critical information element that triggered the decision cycle and subsequent weapons delivery was the electro optical picture or image. At the machine level however, the physical phenomenon that was used to create the image was a photon. A photon is simply a particle of light. The electro-optical sensor on the Digital TARPS POD was sensitive to the wavelengths of light reflected from the skin of the CSSC-3 missile and transporter. The EO sensor counts the number of photons and converts that into electrical signals. The electrical signals are transformed into binary code (1s and 0s) in the digitization process. Once digitized, the information can be transmitted on the network. However these measurements, or raw data, are not human interpretable and must be pushed to processors that convert the measurements back into

various shades of grey or combinations of red, green and blue, and that can be displayed as a matrix of dots of light known as pixels. The aggregation of pixels forms an image that is interpretable by the human eye. The image is stored in some type of file format such as JPEG or BITMAP where it can be presented, manipulated, measured and analyzed. An analyst does not analyze pixels; they analyze the aggregated data product called an image.

The image has information appended to it that describes the content of the pictorial representation in words. It contains the name of the image, the size, time taken, source, or other properties deemed necessary to store, reuse and manage the image over time. This data about the image is called meta-data. Meta-data permits effective management of the image throughout its lifecycle. The image file is stored in a folder or on some form of electronic media such as hard drive or disc, a database or a webpage. From it places of storage, this "data at rest" can be pushed or pulled from computer endpoints onto the network.

From a process perspective, the measurement of the photon reflected from the missile launcher was transformed and stored as a "digital fact" (i.e., a data product called an image). The image was transformed again in a process known as rectification. Rectification placed the image in the context of a pre-defined reference grid that aligned the pixels of the image with actual measurements of latitude, longitude and height above the earth. At this point the image was a "validated fact" and the staff had a measurable degree of confidence that the conclusions they drew from analysis of the image were accurate. The conclusions were then converted into alternative courses of action that were based on the Rules of Engagement, availability of assets and perceived threat. In the scenario, the Admiral had basically three feasible alternatives based on the knowledge he had received from his data collection cycle. He could choose to attack the target, he could choose not to attack the target, or he could request additional information. In this case, the information satisfied his decision criteria and he made the decision to attack the target which resulted in mission success. From a data sharing perspective, although the

details are different, the fundamental steps of tasking, collecting, processing, exploiting and disseminating the information to support this decision cycle are common for most decision cycles.

This was a best case scenario, however. In many decision cycles, the decision criteria are not clear and the existence of data to support the problem may not exist. If it exists, information is often of unknown or dubious quality. Analysts may not be specialists and the decision makers may not guided by clearly defined constraints like ROE. In these scenarios, which constitute most of our decision making, the goal is to cost effectively use data to increase the probability of making decisions that are mission effective and concurrently reduce the risks associated with making bad decisions.

E. DEFINING THE DECISION CYCLE

The ability of data to support consistently effective decision making is dependent on linking the information to a mission or task. If the objectives of the task or mission outcome are ambiguous or unknown, it is difficult to define the decision cycle. Without a decision cycle, decision criteria are difficult to define and the timing of information collection and application cannot be synchronized with the decision maker requirements. Lack of a clearly defined decision cycle confounds systems developers whose job it is to convert human need into executable and repeatable machine processes. Requirements that drive cost effective information sharing leading to mission success must be derived, therefore, from the desired end-state of the task (Loshin, 2007).

The most recent doctrinal articulation of goal-based planning and execution is embodied in the concept of Effects Based Operations (EBO). The first major tenet of EBO is Decision Superiority, and it emphasizes “end-state goals first and then focus on the means available to achieve those goals” (Wikipedia: 2008). Goal-based planning and execution is also apparent in the development of standard operational mission threads which constitute a repeatable chain of events with an objective outcome. A graphic depicting the major functions of the Time Sensitive Strike mission tread is provided in Figure 2-2.

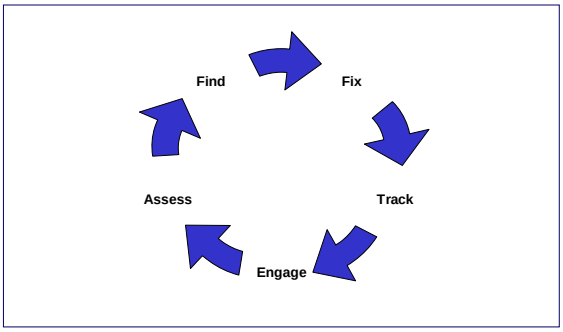


Figure 2-2: Generic Decision Cycle for Targeting Type Missions

Although developed several years after the strike scenario related earlier in the chapter, this diagrammatic view shows that the fundamentals of the mission are relatively stable. This is important for training operators, but more importantly in the context of this paper, it helps constrain the data collection and sharing sub-tasks that will drive the decision cycle. The next chapter discusses the organizational constructs that are evolving that will enable decision cycles and the data required to drive them to be developed and managed across the DoD Enterprise.

III. CHARACTERISTICS OF THE NEW DATA ENVIRONMENT

A. NET-CENTRICITY

Net-centricity is an operational and technical concept that implies optimization of information assets; effectively governing, exchanging, correlating, analyzing and reusing data across multiple data domains to make decisions and achieve mission success. Net-centricity also implies technical requirements for data-level integration and interoperability. These concepts force a cultural change in the way we think and address data usage and management. The primary and most difficult perspective to change is the one relating to scale. In the net-centric environment, data must be managed as an asset across the Enterprise.

Enterprise is a nebulous, subjective term. It tends to confound planners and masks the scope of information sharing responsibilities and functions. In a philosophical sense the Enterprise is a decentralized, global entity which is limited only by the people, processes and technology operating in it, not by any particular organizational construct. For example, the IT data standards that DoD is embracing and building to are developed and approved by international bodies of technicians, scientists and users who collaboratively move the art of the practice forward. World Wide Web Consortium, OASIS, and the Open GIS Consortium are just three examples of these groups that directly affect DoDs data strategy and its implementation. The data that DoD uses comes from an ever expanding global production capacity enhanced by DoD unique sensors, information sources and production processes. Engineering entities spawned from a culture of centralized control, and well defined responsibilities and accountability, such as the one found in DoD, find working in this enterprise disconcerting and difficult.

Conformance to international standards is just one aspect of Enterprise behavior. Figure 3.1 below depicts six major functional areas that must be managed to implement a consistent strategy across very large organizations. The most important aspect of these functions is that they are all based on arbitrary human decisions. This contrasts sharply with other, more traditional, technical fields that are constrained by immutable physical

laws or phenomenon (i.e., gravity, speed of light, magnetism, or human lifespan). Since there are no external, measurable constraints on the way data is defined, produced, managed or used, artificial boundaries are created. These constraints are formulated as definitions, rules, protocols and implementation profiles.

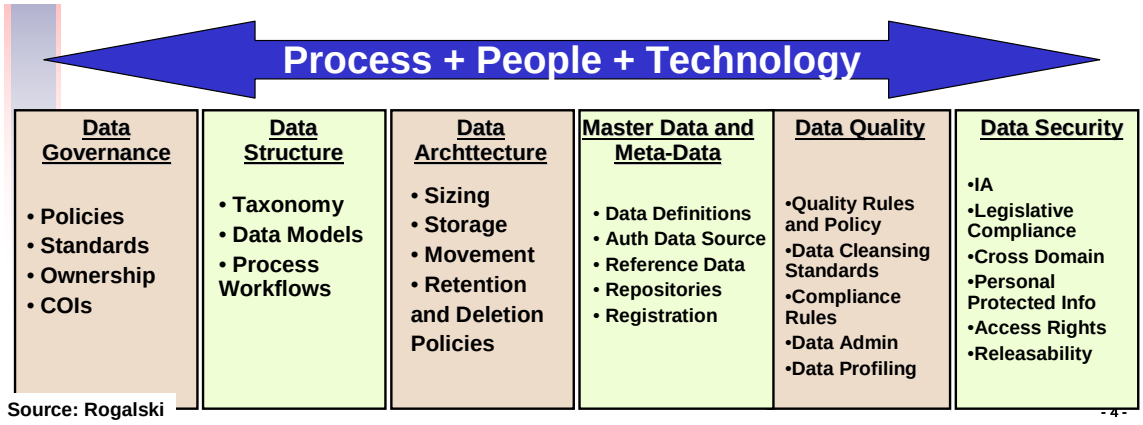


Figure 3-1: Data Strategy at the Enterprise Level (Derived from Rogalski, 2007)

The six categories above represent a static snapshot of many of the activities that occur in an Enterprise. While adequate to describe what functions need to be accomplished, they are not sufficient to define the organization that is necessary to manage the concurrent dynamic processes that constitute data operations in a net-centric environment. One pragmatic conceptual alternative is to execute the data strategy within the data lifecycle management paradigm. This approach to information involves viewing data as an asset that must be managed from inception to disposal, similar to other products that DoD creates or uses. The data lifecycle "begins with a business need for acquiring data. Over time, this data loses its importance and is accessed less often, gradually losing its business value, and ending with its archival or disposal" (Wikipedia 2008).

Net-centricity promises increased operational agility, faster decision making and improved mission effectiveness (Albers et al, 1999). These capabilities are possible because of a convergence of technologies whose interrelationships must be appreciated in the context of a data lifecycle construct. The following paragraph provides a brief

description of the interrelationship of the four basic technical tenets associated with DoD transformation. These tenets represent fundamental changes to the information technology infrastructure and industry best practices that underpin DoD's overall strategy.

SOA: *Migrating to Services Oriented Architectures for application development:*

In the past software applications were constructed as monolithic blocks consisting of several tightly coupled layers. Modifications to any one of the layers affected the other layers. Fundamentally, architectures following the SOA design pattern do two things. They permit the creation of modular, reusable chunks of business logic (e.g., services) that can be orchestrated or choreographed to create new functionality. SOAs also decouple the tiers of application layer from each other so that each tier can be optimized. In a typical 3-tier environment this would consist of a presentation, business, and data tier. A graphical depiction of these concepts is shown in Figure 3.2.

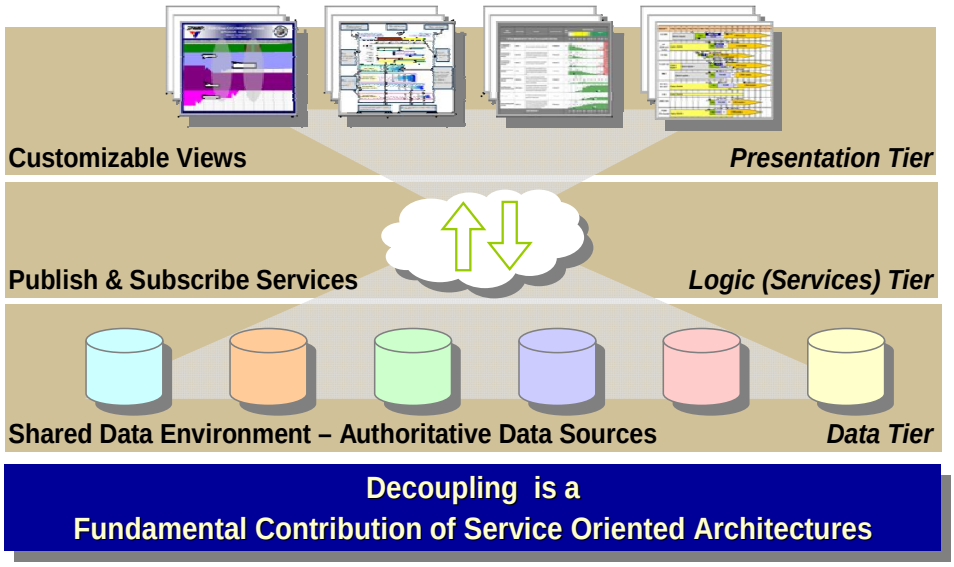


Figure 3-2: n-Tier Application Components (Source: SPAWAR DESC)

Networks / Transport: Migrating from circuit switched to packet switched networking (i.e., from tactical data links to IPV4 and IPV6 networks).

The major innovation with networks is the migration from circuit switched networks to IP, or packet switched, networks. IP based networking permits the

scalability, flexibility and reach of the Internet. When coupled with a Services Oriented Architecture, it permits a highly distributed environment in which services and data can be can be stored and managed in multiple locations and then pulled and configured to support a mission requirement. SOA coupled with IP networking provides the infrastructure for "publish and subscribe" functionality.

Information Assurance: Providing end-to-end security of the network, and providing assurance, confidentiality for data in transit and at rest potentially across multiple security domains.

Information Assurance relates to maintaining confidentiality, access and trust of data on the network and of maintaining the integrity of the network itself. It refers to the classification domains such as Confidential, Secret and Top Secret, their sub-categories (e.g., Secret Releasable To) and increasingly, unclassified access controls. Personally Identifiable Information (PII) and Controlled But Unclassified (CBU) caveats are some of the most recent categories of data for which information assurance rules are being modified and strengthened within DoD.

Data: Making data visible, accessible and understandable on the network through meta- tagging with the XML family of standards and posting to shared space.

In traditional acquisition programs and monolithic software application development, data is an integral part of the system and tightly coupled to it. The syntax (e.g., structure) and semantics (e.g., meaning) of data are tailored to the requirement of that system the program manager for the system is responsible for the data definitions and flows within the system. While the networks provide connectivity and services supply the application logic, capability improvements associated with the network centric environments are manifest in the fact that data assets can be loosely coupled to other components of the infrastructure and can be managed dynamically as a component of warfighter specified mission areas. The concept of data level integration refers to the ability of computers to understand the meaning and relationship between various shared data elements.

B. INFORMATION REQUIREMENTS

In the legacy environment, information exchange requirements and required data qualities could be predicted adequately. Department of Defense Architectural Framework (DoDAF) views allowed systems developers to define their Information Exchange Requirements (IER) which drove system design. In the environment described above, the concept of static information exchange requirements between nodes in system's architecture is no longer valid and new architectural methods are being investigated to augment or modify the DoD Architecture Framework (DoDf, 2007). In fact one of the most attractive aspects of the Services Oriented design pattern is the ability to support "unanticipated users," those people, organizations and processes that have a need for data but whose need could not be predicted by either producer or consumer at system design time. These needs arise from dynamic conditions of real world operations.

C. DATA QUALITY AND VALUE

The tradeoff between flexibility and predictability remains a difficult decision as DoD evolves into a net-centric environment. If information exchange requirements drive system design but can no longer be predicted, what now triggers the processes needed for development? It is possible that a level of information readiness can be defined that permits data producers and infrastructure sustainers to create and maintain conditions where high quality information exists and can be invoked upon demand.

During his long tenure as the Chief of Naval Operations, Admiral Vern Clark tasked his staff to improve readiness "but not at any cost" (Clark, 2000). He directed that navy missions be viewed from a business perspective and reminded those of us on his staff that businesses can't long afford to be sloppy with their working capital or they cease to be viable. Over the past eight years the Navy has adopted many industry practices to try to reduce cost while maintaining both current and future readiness. The promise of Network Centric Operations is that information can be cost effectively applied to decision making so that physical assets like ships, aircraft and humans can more effectively execute the wide variety of DoD missions. Much time, effort and funding has

been expended on improving connectivity; creating the network infrastructure that provides the capacity to share information. Five years ago, DoD policies started to reflect the need to focus more attention on managing the content on the network to stem the growing problems of information overload and chronic bandwidth limitations.

These policies, starting with the Net-centric Data Strategy in 2003, recognized what industry had already learned, namely that the key to success was the ability of content providers to reach end-users through the infrastructure backbone provided by the internet (i.e. Internet Service Providers). More specifically, capability was achieved through the ability of content providers to add value in the context of the end-user defined processes. Since the cost of managing data throughout its lifecycle is largely independent of the data's utility, efficiencies must be gained by initiating the lifecycle only for useful data. Industry uses the term Master Data to reflect information critical to business processes. In DoD a similar concept is reflected in the term Authoritative Data Sources (ADS) (SECNAV, 2005). Authoritative or Master Data is defined by quality attributes which can be incorporated into the data asset as metadata. Each quality attribute provides some arbitrary level of value that is based on mission or business context. David Loshin provides a simple graphical illustration of the line of questioning that must accompany the designation of master or authoritative data in Figure 3.3 below.

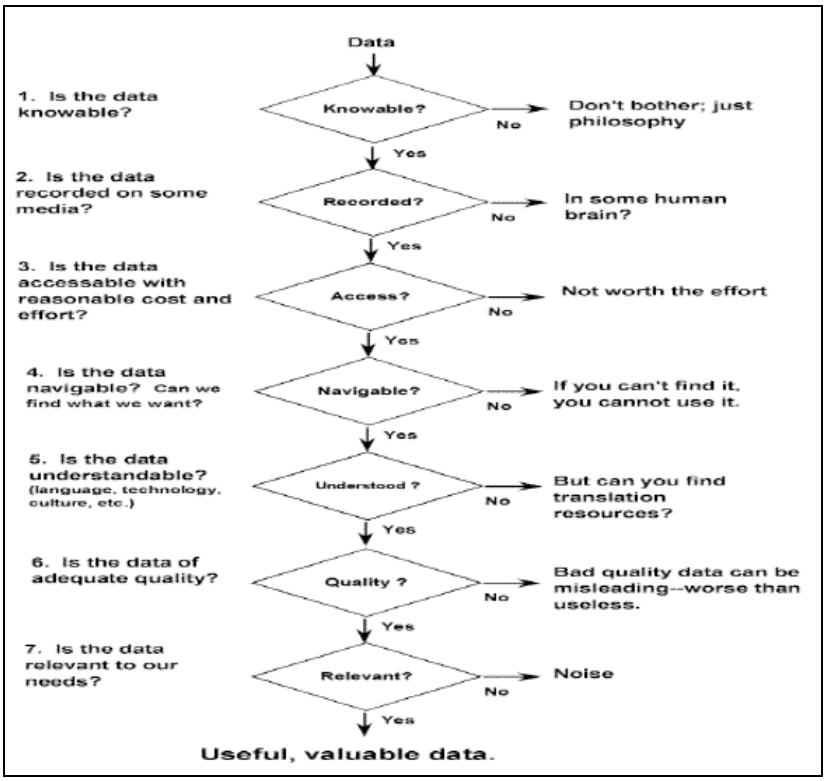


Figure 3-3: Notional Decision Tree for Data Quality Assessment

Although technology makes increased operational flexibility possible, defining authoritative data requires a great deal more planning, discipline and data governance than was necessary under data management regimes in the past. DoD uses Technology Readiness Levels to determine the maturity of emerging technologies and the risk associated with incorporating these technologies into a DoD design. DoD also uses operational readiness levels to provide leadership a metric on the current capability of the operational forces under a commander's control or authority. If we are to treat data as an asset, it is necessary to create readiness levels for data that can provide a meaningful level of risk reduction and situational awareness for operational commanders.

A notional Information Readiness Levels matrix is included Figure 3.4 below. It derives concepts from Joint Publication 6.0 "Joint Communications" which describes eight quality criteria associated with the value of data; visible, accessible, understandable, trusted, interoperable, timely, relevant, accurate. The first four qualities are primarily technical in nature and the last three are more operationally focused.

Information Readiness Level	Description
1	Visible, Accessible, Understandable, Trusted, Timely, Relevant and Accurate Information is available to perform this mission.
2	Visible, Accessible, Understandable, Trusted information is available to support this mission.
3	Information is Visible but it is not accessible
4	No information can be discovered to support this mission
Information Qualities	**Definitions**
Visible	Information is advertised on the network (Tagged and registered)
Accessible	Stored in a shared space on the network
Understandable	Human and / or machine readable
Trusted	Relates to the authority and security of data
Interoperable	Ability to exchange information
Timely	Available in time to make a decision
Relevant	As it applies to a specific mission
Accurate	The data conveys the truth at the required level of precision

Figure 3-4: Notional Information Readiness Levels

D. RISK REDUCTION

One of the implied assumptions in DoD net-centric theory is that data sharing is inherently good. In 2002 the Assistant Secretary of Defense introduced the concept of Task, Post, Process and Use (TPPU) that replaced the traditional Task, Collect, Process, Exploit, Disseminate (TCPED) process model (U. S. Joint Forces Command, 2004). By providing a broader range of data to more potential users earlier in its lifecycle, this new process model was designed to reduce the decision cycle and improve the ROI of the information sharing investment. However in environments flush with information, TPPU, without the appropriate data quality attributes to provide some degree of volumetric filtering, becomes problematic. In a byline entitled the "The Too-Much Information Age" SEED magazine editors predicted that "the sum of all information produced in 2008 will likely exceed the amount of information generated by humans in the past 40,000 years" (Bly, 2008). The article goes on to state that there is an inverse relationship between the amount of information collected and level of knowledge

derived. This is because critical thinking is required to turn knowledge into action and there is just not enough human time available. This assertion is reinforced by Bloom's Taxonomy of critical thinking depicted below. Knowledge is the lowest level and the foundation for critical thinking. The taxonomy culminates with Evaluation which is defined as "presenting and defending opinions by making judgments about information, validity of ideas or quality of work based on a set of criteria" (Barton: 1997). Evaluation then becomes the level at which consistently good choices between alternatives can be made and the therefore the level that is the objective end state and the focal point of our information technology investment.

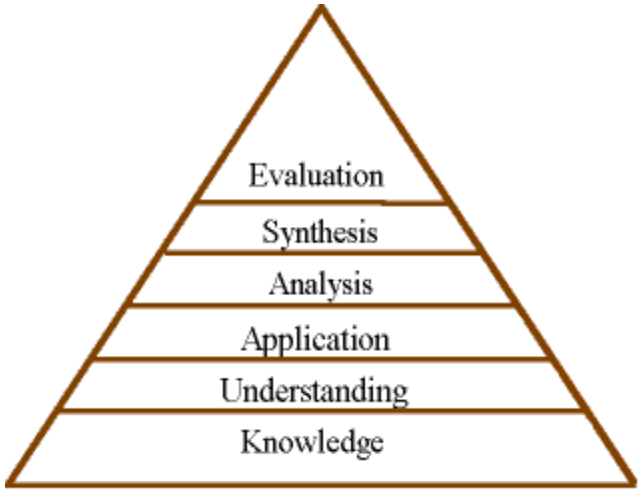


Figure 3-5: Bloom's Taxonomy

As stated in Chapter II, to achieve decision superiority, the information technology architecture must be continuously groomed to aggregate, fuse, distill and present information at a human consumable rate. According to Wikipedia the field of Knowledge Management formally emerged in 1995 to respond to the need for more symbiotic relationship between information management and information use. The Knowledge Management field has broadened to include a wide range of loosely related sub-disciplines with no formal definition (Wikipedia 2008). Knowledge Management has become a cliché for any information management approach that improves the usability of data and capturing human experience with it. In a strategic sense, Knowledge

Management is an attempt to collect, categorize, store and reuse a theoretically ever expanding volume of facts and figures contained in voice, video and text formats.

When applied to practical decision making, Knowledge Management can become a reactive tail chase resulting in an endless pursuit of new data to make the "best" choice. In his book "Risk Analysis in Engineering and Economics," Bilal Ayyub suggests that:

> Information abundance does not necessarily give us certainty. In fact this abundance of information can sometimes lead to errors in decision making and undesirable outcomes due to either overwhelmingly confusing situations or a sense of overconfidence that leads to improper use of information. (Ayyub, p.1)

Professor Ayyub suggests that in an era of information abundance, "engineers and scientists emphasize knowledge and information, and intentionally or unintentionally brush aside ignorance" (Ayyub, p.16). A focus on ignorance reduction rather than knowledge attainment can lead to efficiency. Wikipedia defines ignorance management colloquially as "discovering what we need to know, but don't." This is an extremely useful concept for decision making because it inherently deals with risk and risk reduction. Knowledge management more appropriately pertains to researcher and analyst functions rather than decision making activities. In a practical sense, ignorance management involves collecting enough data to reduce risk to an acceptable level, or decision threshold. It involves epistemological concepts such as uncertainty, complexity, ambiguity and equivocality. In the context of military decision making, an approach to based on reducing ignorance appears consistent with General Colin Powell's points for good leadership where he recommends "Once you are in the 40-70 percent range (of information collected) go with your gut" (Powell, 2008).

Ignorance management implies you know what you don't know. It also implies there are known qualities for the data that you are trying to collect and the decision maker will recognize and understand the data when it is presented. In the ignorance management paradigm, data collection and analysis is terminated once the decision has been reached. In a knowledge management scenario, there is the potential to never reach a data collection termination point. If the decision thresholds are well defined, data

collection, analysis, and use can focus on achieving these thresholds. This focus on the decision quality data and decision thresholds permit the information architecture to be more effectively groomed to deliver the "right information, to the right person at the right time," and can help control the total cost associated with information management.

E. IGNORANCE MANAGEMENT AND SLA

Attainment of the operational condition known as Decision Superiority assumes that there are competent/rational decision makers with the information and authority and will to make decisions. While there are many decisions made based on experience, in a military operation or complex business relationship, decision support tools are often used. In the non-net-centric environment, decision support tools are pre-designed and the information interfaces are static. In a net-centric environment, the ability to orchestrate services and data create a dynamic tool suite that is more tailorable to changing operational conditions. As operational conditions change, decision thresholds change, and these changes alter the qualities of data and the reliability of the tool suite needed by the user. One of the instruments used by the telecom industry to provide various levels of performance to changing conditions or different operational priorities is called the Service Level Agreement (SLA). Wikipedia (2008) defines SLA as, "A formally negotiated agreement between two parties." It is a contract that exists between customers and their service provider. It records the common understanding about services, priorities, responsibilities, guarantee, collectively known as the level of service. For example, it may specify the levels of availability, serviceability, performance, operation, or other attributes of the service like billing and even penalties.

Service Level Agreements pertain traditionally to the qualities of the network itself or the availability of the services (e.g., applications) that ride on the network and are often rendered as a Quality of Service requirement. Sid Frank in a 2006 article entitled "Service Level Agreements for Data" responded to a need by the financial services industry to more effectively monitor and control the quality of data they were receiving from 3rd party data producers. Mr. Frank indicated that the SLA for Data (SLA4D) should include data quality metrics, formats and provider quality certificates (Frank, 2006).

These requirements and solutions are applicable to the DoD net-centric environment as well, where poor quality data introduced into fundamental processes could also be costly or catastrophic (Frank, 2006). The net-centric paradigm essentially creates a class of government entities who serve as 3rd party vendors that constitute the data production capability for many mission areas.

The discussion of data quality in the context of service level agreements has yet to begin in earnest in DoD and the concept of contracts for SLAs between systems, DoD or government agencies is an emerging field of study. As the infrastructure matures, more services become available and more data exposed for reuse, the problems and solutions Mr. Frank discusses will become more applicable. In parallel to the infrastructure maturation, a comprehensive dialog on the concept of Information Readiness Levels as a quality measure, ignorance management as a risk reduction technique and SLAs for data should be initiated to support precision data operations for decision support.

F. FUNDING THE DATA LIFECYCLE

In order to reduce costs, gain networking efficiencies and improve mission success the fiscal resource bureaucracy must evolve to accommodate the new more dynamic requirements that decision makers will place on the IT infrastructure. The modification to budgeting systems must address the de-aggregation of traditional systems into components and the need to finance layers of the SOA n-tier environment.

The defense acquisition process is driven by mission needs. The Planning Programming Budgeting and Execution process is keyed to respond to these needs by funding programs and projects whose functionality is defined in terms of systems requirements. In the DoD acquisition model, systems defined by these requirements are developed, managed and funded independently from one another. These systems are the "products" that DoD creates (i.e., ships, airplanes, radios, sensors, missiles, satellites, software applications, networks). For most systems, data is a byproduct of the successful execution of the acquisition process. That is, the need for data creation and management is a consequence of a system performing its intended function.

The cost of data is partially accounted for and resourced within the total lifecycle cost and total obligation authority of systems that consume or produce data. Any system that contains software (i.e., microprocessors and associated circuitry) contains data and all but the most rudimentary of systems contain some software. Gas masks and 9mm pistols fall into this category. When the data that a system uses is produced and consumed within a system's physical boundaries, the cost of that data can be accurately predicted and resourced from within the system's budget. This can be thought of as a closed system. However, when a system uses data from another system or produces data for another system to consume, the boundaries are breached and the cost estimates relating to those data exchanges become harder to predict. From a management standpoint, the responsibilities for the lifecycle costs of data are now shared between the producing and consuming nodes. Unfortunately, current acquisition theory and practice do not deal effectively with this fiscal no-man's land. According GAO Cost Assessment Guide, costs have proven so difficult to predict accurately that integration is one of the main factors in budgetary shortfalls and cost overruns for many major defense programs (GAO, 2007).

One attempt to realign the resources with DoD's emerging transformational needs was the creation of Portfolio Managers. The next chapter will briefly discuss Portfolio Management and focus on the organizational changes related to data and services management in the portfolio known as Communities of Interest.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PORTFOLIO MANAGEMENT AND COMMUNITIES OF INTEREST

A. PORTFOLIO MANAGEMENT

Transformation of the Department of Defense into a net-centric enterprise required fundamental changes to the information technology (IT) management paradigm. This shift is clearly reflected in DoD Directive 8115.01, "Information Technology Portfolio Management" that mandates that IT investments would no longer be managed and funded as individual systems but as portfolios. The Directive defines a portfolio as "a grouping of IT investments by capability to accomplish a specific functional goal, objective or mission outcome" (DoD, 2005).

The Directive defined and established the Enterprise as the DoD and described roles and responsibilities for newly designated portfolio managers. The Enterprise was decomposed into the following four mission areas representing fundamental capabilities: Business Mission Area; Warfighter Mission Area; Enterprise Information Environment Mission Area; and DoD Intelligence Mission Area, e.g., BMA, WMA, EIEMA, and DIMA respectively. Each mission area lead has the responsibility to analyze, select, control and evaluate systems, programs and projects within the portfolio to optimize capability, limit redundancy and reduce overall cost to the government (DoD, 2005).

The Directive was followed one year later by DoD Instruction 8115.02 entitled "Information Technology Portfolio Management Implementation." The purpose of the instruction was to support changes to the Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System, and the Planning, Programming, Budgeting and Execution Systems (PPBE) that were also part of the DoD's transformation initiative. The portfolio management process was designed to "continue the evolution from an emphasis on individual systems to overall mission capability" (DoDd, p. 4). Figure 4.1 depicts DoD Mission Areas and their relationships to the Joint Capability Areas. Initially, the 8115 series was generally viewed as one more enigmatic aspect of DoD transformation, however each Service retained control of their funding

lines. Fiscal Year 08 Program Objective Memoranda (POM) submissions that were being developed were not evaluated from the new portfolio perspective. However, by PR09, Commands, Services and Agencies were all attempting to align with the new directives. In the FY10 POM cycle, portfolio managers have started to exercise investment program oversight, including attempting to gain influence over the decisions to "start, continue, modify or terminate programs" (DoD, p.12).

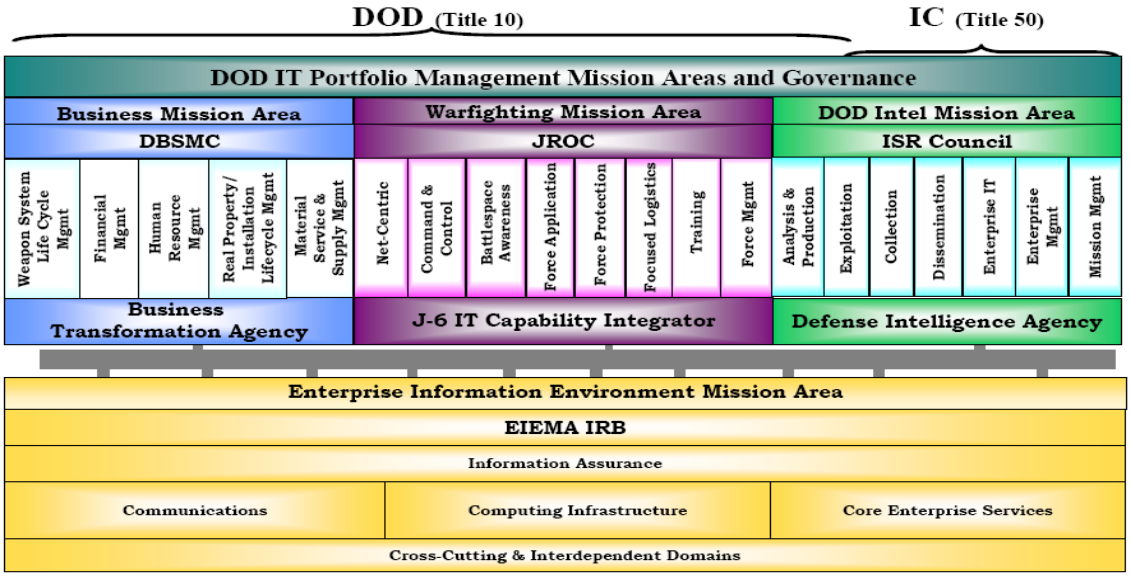


Figure 4-1: DoD Mission Areas. (Source CJCSI 8410.01)

In addition to supporting execution of the newly refined decision support systems (e.g., JCIDS, DAS and PPBE), portfolio managers, mission area leads and sub-portfolio authorities' execution have explicit responsibilities for implementing DoD Directive 8320.02, "Data Sharing in a Net-centric Department of Defense." Specifically the responsibilities include (1) facilitating information sharing within and across Communities of Interest, (2) Identifying the highest priority data sharing needs, (3) designating a component lead for COIs and, (4) defining data strategy implementation metrics.

B. DATA SHARING AND PORTFOLIO MANAGEMENT

DoDD 8320.02 states that data is "an essential enabler of network-centric warfare (NCW) and shall be made visible, accessible, and understandable to any potential user in the Department of Defense" (DoDb, 2004). This Directive represents one cornerstone of defense DoD transformation efforts. All other transformational directives, instructions and technical implementations, and arguably the concept of the Global Information Grid itself, are fundamentally dependent on the ability to find, move and correctly interpret data.

DoDD 8320.02 attempts to address limitations of data regulation efforts embarked on by DoD in the early 1990s and codified in DoDD 8320.1, "DoD Data Administration." That policy attempted to standardize all data elements across DoD. This effort led to the development of massive data models that relationally organized a great deal of DoD knowledge but could not be used effectively for sharing data. Developers were forced to tailor the mega-models to meet their data sharing requirements and reduce the complexity of implementation. As computer systems tailored the models differently, they could not exchange data, and information flows had to be augmented through some form of translation or mediation.

The concepts of visibility, accessibility and understandability were introduced previously in Chapter III as data qualities that could be measured or gauged to define information readiness levels in the context of operational scenarios. DoDD 8320.02 and its associated implementation guide, DoDI 8320.02, provide guidance and define roles and responsibilities for DoD to engineer the conditions that will achieve the objective operational state. Engineering here is used in its broadest sense to include the social, procedural and technical aspects of designing, building and implementing the net-centric Enterprise data architecture.

C. COMMUNITIES OF INTEREST

Communities of Interest (COI) have emerged at the heart of net-centric data strategy. They represent a fundamental shift from localized data management, to a wider infusion of roles and responsibilities focused on governance. Communities of Interest are defined as:

> Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange (DoDb, p.4).

COIs are designed to reduce the standardization dilemma by breaking DoD into smaller data domains that can be managed by the mission areas or portfolio managers. The concept has matured sporadically over the five years since they were initially defined in the DoD Net-centric Data Strategy but their importance has continued to grow at a steady pace as the Department evolves its infrastructure toward web-based paradigms.

A number of factors have contributed to the modest rate in which COIs have been embraced. First, there appears to be a lack of understanding of the basic concepts and functions that COIs are designed to perform. COIs migrate key data engineering responsibilities away from the acquisition community toward the business user and operational mission practitioner. End users are being exposed to data management principles that they previously took for granted and had dealt with as "black boxes" within the Information Technology realm. Day-to-day experiences with Google and other technologies that have facades of simplicity probably contribute to a pervasive misunderstanding of the complexity of harmonizing heterogeneous datasets.

Secondly, COIs reside in a fiscal no-man's land. COI products and activities affect many programs of record and exist at an enterprise management level that is evolving and currently co-existing with traditional Title 10 resource sponsor responsibilities to "man, train and equip" the operational forces. Resource sponsors have difficulty justifying investments that are not unambiguously related to Programs of Record or organizational operations. The establishment of the portfolio management construct is part of the remedy for this problem but, the concept is young and the processes and authorities of the portfolio leads are still being tested and defined (CJCSb, 2007). Even within the portfolio construct there are necessary fiscal boundaries that must be defined. COIs are inherently collaborative in nature and resource sponsors are reluctant to commit resources to activities that are beyond their formal control, oversight and accountability.

Finally, the migration toward COIs appears to have been actively or unintentionally hindered by data administration professionals, data modelers, recalcitrant government program managers and industry vendors who may have vested interests in maintaining the status quo. When asked why, one senior data strategist quipped, "…because there is profit in chaos." Data sharing in a net-centric environment violates the basic business tenet of "design once, sell many" and supplants it with the less profitable model; "build once, use many … for free." The technologies being exploited in a net-centric environment are requiring companies, developers and their government sponsors to learn and implement quickly (Dartmouth, 2007).

D. 10 STEPS

Unfortunately, the definition of COIs contributes to some of the confusion. Based on the explicit and implied roles and responsibilities in the Directive, there is a substantial engineering and development element to COI. In most COIs this is accommodated in a sub-group to the COI that reports to the COI leadership. Integrated product development teams are responsible for establishing metadata structure, defining community ontologisms, establishing shared space and cataloging data (DoDb, p.5). These are not traditional user roles and can stymie COI establishment early in the organizational lifecycle.

In an effort to socialize and explain the tenets of COI to a broad Navy audience, my colleague Paul Shaw and I developed a brief entitled the "First 10 Steps" for COI development. The introductory slide to that brief is shown in Figure 4.2. The brief was used in 2006 and 2007 to help bound the COI issue, educate ourselves and our colleagues and assist others who were attempting to implement or comply with DoD policy. At the time Paul was one of the advisors to the Maritime Domain Awareness and many of the lessons learned came from his participation in the Data Management Working Group established to support that Northern Command (NORTHCOM) led effort.

Figure 4-2: COI First 10 Steps

After the COI is established and the products are developed and validated through piloting, the COI is faced with influencing the acquisition community to integrate the products in programs of record that will sustain capability and deliver it to end users.

E. CROSS COMMUNITY SHARING

Although there was a collective desire to establish communities of interest and mature them to support development teams and end users, few of the initial COIs that were identified and registered in 2004 remain active. As of June 2008 only 30 of 170 COIs have created and registered artifacts in the DoD Metadata Registry (MDR, 2008). Of the COIs that did begin to meet and develop artifacts, various new challenges arose as the individual data domains attempted to support a user base that was simultaneously executing multiple missions. The dearth of personnel that had experience with web services, data modeling and the concepts of enterprise-level problem solving ensured a chronic understaffing of these efforts. This resulted in a small set of government engineers, Federally Funded Research and Development Corporations (FFRDC) and

defense contractor support personnel who worked multiple COI efforts, shared lessons learned and carried attitudes, perspectives and data management working groups.

Each COI had a different learning curve and entered into the COI development process at different levels of maturity. They also had different levels of political commitment and high variability in their funding availability. In an effort to adjudicate issues between COIs and more formally share lessons learned, OSD NII established the CIO Forum in 2006. One of the first issues taken up by the COI Forum was the problem relating to cross-COI interoperability. Although the COIs were implementing the same policies and using the same standards, cross-COI harmonization was not occurring. There was a potential therefore of creating new stovepipes of net-centric data which when implemented, would fall short of the conditions needed for net-centric operations to occur. Interoperability would require layers of mediation or mediation services between COIs to achieve the desired level of machine-to- machine interoperability.

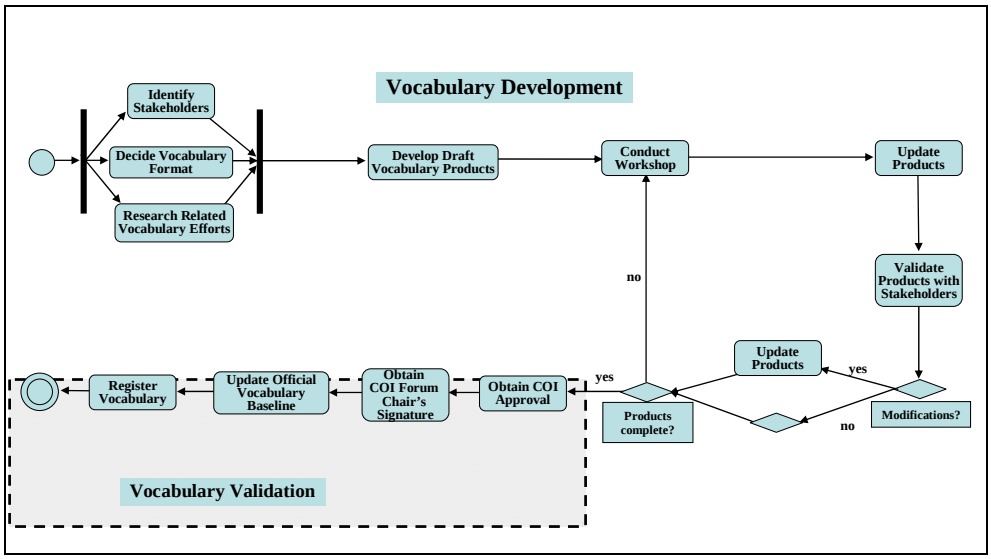


Figure 4-3: Vocabulary Development Process (Source: COI Forum Brief, 2007)

Figure 4.3 depicts one of the principle processes that the COI Forum generated and endorsed. The workflow is a simple graphical representation of the steps and relationships that a community would go through to define itself, the vocabulary it desired to share and the mechanism to make it discoverable to others in DoD. What the workflow is unable to depict is the tremendous amount of time and effort required to

form a community, and the degree of leadership, follower-ship, administrative overhead, and collective goodwill required to come to agreement on the lexicons and their relationships.

At the same time DoD was striving to increase the slope of its net-centric learning curve, other departments in the federal government were under similar pressures to improve interagency interoperability and reduce overall investment in IT. This had been a thrust from Congress and the Office of Management and Budget since the late 1990s, but the events of September 11, 2001 and the subsequent 911 Commission Report findings changed that desire for interoperability to a national mandate and strategy (National Security Council, 2007).

The Federal approach to data sharing is incorporated in the Federal Enterprise Architecture (FEA) created by the Office of Management and Budget. The Architecture is comprised of a collection of interrelated reference models designed to facilitate cross-agency analysis to help identify duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies. The components of the FEA are shown in Figure 4.4.

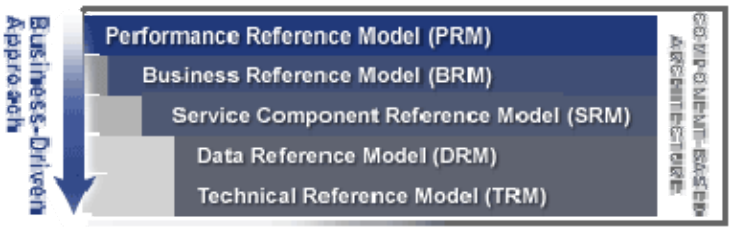


Figure 4-4: Federal Enterprise Architecture (Source OMB)

F. DATA REFERENCE MODEL

IEEE 610.12-1990 defines a model as "an approximation representation, or idealization of aspects of behavior, operating or other characteristics of real world processes, concepts or systems" (Maier and Rechtin, p.145). The Data Reference Model

(DRM) reflects the same technical and organizational considerations for data sharing as those reflected in DoD directives. OMB intends for the DRM to be used by federal data and system architects to describe information in such a way that it can be easily located and used across multiple federal agencies.

Models can be helpful in defining abstract concepts related to network centric theory and describing enterprise behaviors. The data reference model provides high level, implementation neutral guidelines for enterprise data management. It is composed of defining vocabularies, placing data in context and sharing data. The document describes in detail the reasoning behind each of the three main concepts and how they relate to each other. The DRM describes how COIs should define their vocabularies as hierarchical taxonomies to facilitate classification of data which then allow alignment based on the context of the Mission Area or Line of Business (LOB). Alignment within DoD refers to mapping the lexicons to the Mission Areas and Joint Capability Areas as displayed in Figure 4.1.

G. RESULTS OF COLLABORATION

COI collaboration eventually spawned a hypothesis that cross-domain interoperability could be built into the CIO data artifacts if the most commonly used terms could be defined and used as a starting point for data taxonomy development. It was an attractive argument that promised to improve consistency of implementation and facilitate the development of a data interoperability design pattern. The concept became known as the Universal Core.

In an effort to capitalize on the political, technical and cultural momentum that had developed the DoD Chief Information Officers, the Intelligence Community chartered a short duration study in January 2007 to evaluate the feasibility of defining and creating the Universal Core as a reusable information exchange standard and implementation profile. The next chapter describes the evolution of Universal Core in the context of a federal Community of Interest case study.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY: UNIVERSAL CORE

uni·ver·sal: ***Adjective***

- Embracing a major part or the greatest portion.

- Adapted or adjustable to meet varied requirements.

Merriam-Webster Online Dictionary (2008)

A. ORGANIZATION

In January 2007, the Office of the DoD CIO and the Intelligence Community CIO, in their roles as co-leads for the Senior Enterprise Services Governance Group (SESGG), established the Common Core Task Force that was chartered to evaluate the concepts of data sharing defined in Federal policy and to evaluate the various efforts that were ongoing in the Federal government at the time. This resulted in an unpublished February 2007 report entitled "Criteria for Universality and Utility of Information Structures" (CCTF, 2007). The report noted that the "traditional mindset of meticulously documenting information exchange requirements clearly does not deliver the type of business process agility" required for interagency partnering and data sharing. The report went on to theorize:

> One approach to mitigating this problem is to adopt existing agreements on semantics and syntax for concepts that are universal (or at least broadly common), thus forming a "Universal Core" of implementable objects that will be used in information systems wherever practicable (CCTF, p. 8)

In April 2007 as a follow-up to the report, the SESGG established the Universal Core Working Group. The charter was broadly described to provide the working group the opportunity to evaluate best practices in government and industry. The primary tasks of the working group were to define those vocabulary terms that could be considered fundamental to all information exchanges, gain consensus on the terms by the various departments and agencies within DoD and the IC, and implement the vocabulary as an

information exchange specification. The Office of the DoD CIO tasked Navy to lead the effort. I was assigned the working group lead for DoD and the co-lead was designated from the Office of the Director of National Intelligence, Mr. Jim Feagans. This effort was to be completed by the end of fiscal year 2007. Typical for this type of IPT, no funding was provided, no labor was dedicated to the effort, and the co-leads were not relieved of their existing responsibilities. Despite these challenges, the allure of establishing a small, lightweight information exchange specification that would serve as the foundation for COI and cross departmental interoperability was enough to maintain senior level interest and technical level participation.

B. MISSION AND OBJECTIVES

The Common Core Task Force Report served as the foundation for the initial working group objectives. The paper provided a broad conceptual definition of Universal Core and some design tenets that served as the underpinnings of the concept. The Common Core Task Force defined Universal Core as "the set of concepts that require no domain-specific expertise for understanding, i.e. a set of things that anyone can understand" (CCTF, p.4). They went on to define a Universal Object as "an implementable specification of syntax and semantics" of the universal terms defined above. The tenets were modified to express more concrete themes that could be used to define and scope working group deliverables:

- The benefits of a Universal Core framework will occur when everyone can agree on and implement the fundamentals.
- The specification must be documented and technically implementable so that developers can code against it and program managers can put it on contract.
- Extensibility is considered an essential quality. However, it does not mean that the core itself is changed by any extensions.
- Implementation must be cost effective.

C. INITIAL CHALLENGES

As requirements, these definitions and tenets constituted very broad vision statements. Although UCore was to be defined as a technical specification, the first challenges were philosophical in nature. In order for the Core to be considered truly universal the concepts and terms in the core had to be context free. That is, they had to be defined and represented in a way that every data domain and Community of Interest could use them. Since the working group had a broad charter, it was able to evaluate all previous data sharing initiatives and to deduce what was common among them. Analysis by MITRE Corporation determined that almost 80 percent of all tactical message traffic (i.e., Link 16) contained the primary concepts of "who," "what," "where" and "when" (MITRE, 2006). These fundamental concepts were first introduced to western philosophy by Aristotle, are the foundational concepts for journalistic writing and serve as the basis for intelligence community reporting. Other data sharing initiatives such as Cursor on Target and the Strike Community of Interest had started to define these basic concepts as part of their taxonomies although they did so in the context of their specific mission areas.

Ultimately, time and resource constraints forced the working group to reduce the initial scope of the project to defining only two abstract concepts of "where" and "when." These are the terms that could be most easily defined in terms of "location" and "time." Location and time are also formally represented in Geographic Markup Language and ISO 8601 respectively. Additionally the group believed that the political payoff resulting from the two primary stakeholders agreeing to anything outweighed any desires by the group to accept the risk of trying to include all four terms.

The next major challenge that was addressed by the working group dealt with the syntactical representation of the vocabulary terms. Prior to the definitions being agreed upon, data modelers and designers were reluctant to choose a single physical model for fear of being boxed in for future development. The major point of contention between the various experts was whether to specify XML in a physical instantiation called an XML Schema Description (XSD) or leave the physical modeling up to the

implementation teams. Vociferous debate occurred between PhDs who were veterans of the Artificially Intelligence community and continued to conduct advanced research on the emerging semantic web and other WEB 3.0 concepts. In the end the co-leads refocused the debate on what could be feasibly implemented during fiscal year 2007 and what the overall cost to the government would be for implementation. XML was chosen as the logical representation for the concepts with the physical schema being represented in XSDs.

Organizing for effective operations was the next obstacle. The co-leads were geographically displaced by 3000 miles in San Diego and Washington DC respectively. The volunteer technical workforce was distributed throughout the country. This necessitated design meetings being conducted primarily through teleconferencing. Initial meetings were large and many of the participants were attending in a defensive role to protect their organizational equities rather than contribute meaningfully to the effort. These interested onlookers distracted the government, technical and subject matter experts who were actually engaged in meaningful work. In order to improve efficiency, the co-leads created sub-groups that were limited to those who, through peer review, had demonstrated a clear understanding of XML, data modeling techniques, web services and an understanding of the political goals of the project. In time the draft products from these subgroups were vetted to the larger community for review and official comment.

The technical task of defining a few common terms in XML, documenting the meaning (i.e., semantics) and formatting (i.e., syntax) are not complex and could be done in a reasonable time by two or three developers. However, since the goal of Universal Core was interagency adoption, the SESGG mandated that the design team meetings be unrestricted and widely advertised. Although face-to-face meetings were difficult to organize, three of these were conducted and proved invaluable to maintaining the project on schedule. Teleconferencing is an excellent, cost effective tool but it is not substitute for the human interaction that builds loyalty, trust and team spirit.

The co-leads hosted the first meeting at MITRE facilities in Mclean Virginia the third week in July 2007. Forty five individuals representing over 20 organizations within DoD and the IC attended. Although well organized with timelines and subgroup

deliverables, the event was a frustrating failure for the co-leads as well as the participants. It resulted in little more than an introduction to the Universal Core and a venue to air grievances from previous data sharing initiatives. The decision was made to end the meeting at noon on the second day when it appeared that meaningful progress was unattainable.

In an attempt to render some form of progress from an otherwise stalled initiative, the co-leads invited a handful of colleagues to a small conference room to strategize the way ahead. The individuals were picked for their ability to objectively advise the government, their reputation within the data community, and their experience on other Communities of Interest. The meeting lasted four hours and by the end of it, a reasonable plan of action and milestones (POAM) had been drafted, vocabulary terms and some attributes had been defined, data standards had been prioritized, challenges identified, and tasks assigned. That meeting was the galvanizing event in the entire UCore effort. To the co-leads it served as an epiphany that the Universal Core initiative, and data sharing in general, is primarily a human endeavor supported by a technical component.

The UCore team worked through August via weekly developer teleconferences and almost daily conversations by the government co-leads. The data engineers reported out in the third week in August that they would be able to define and build the implementation profiles for the concepts of “when” and “where” that would be conformant to policy, consistent with international data standards and valid in the context of XML parsing tools. The government was in a position to be able to deliver a product to the oversight body that could be called the Universal Core that would conform to the tenets of the original SESGG tasking.

One final face-to-face meeting was called in early September to review the artifacts, assumptions and political considerations of the effort. The month of September 2007 was devoted to creating a Development and Implementation Guide (DIG) for Universal Core Version 1.0. The DIG contained and background on the UCore effort, guidance on how to build and extend UCore artifacts in order to tailor them to specific mission needs and examples XSDs to guide implementation. The government

leads reviewed the artifacts and agreed that the effort had produced a valuable, but limited, information exchange specification. They made the decision to present UCore to the SESGG recommending UCore not be released for implementation but be used as an example of government, industry, academia partnering and the ability to collaborate on technical standards. They also recommended the immediate initiation of UCore V2.0 to be developed and implemented in Fiscal Year 2008. The update slide in Figure 5.2 below was presented as part of a status brief to DoD CIO representatives on 27 September and provides insight into the status of the effort and government concerns and goals for the initiative.

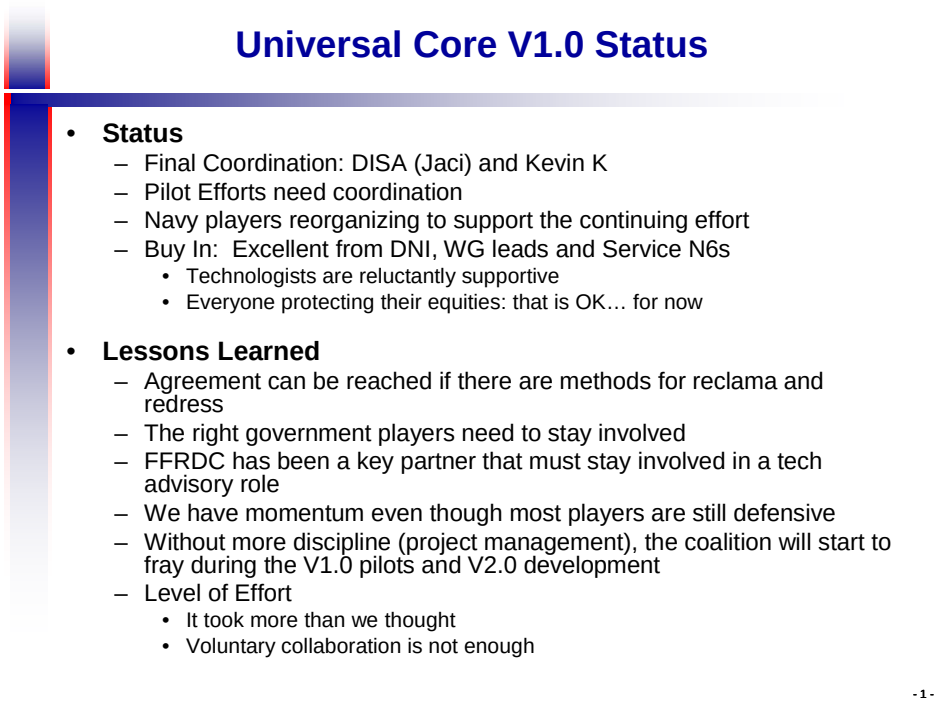


Figure 5-1: UCore V1.0 Status. 27 Sep 2007 Brief to OASD NII

D. RESULTS AND REACTION

Universal Core V1.0 was released for DoD and Intelligence Community review the week of 04 October 2007. It was hailed immediately by DoD and IC leadership as a success. Politically, the teams had come together, overcome cultural and organizational barriers, and produce a joint technical product. The UCore initiative proved that there

was latent capability previously funded by the DoD and IC that could be leveraged to support mission accomplishment. It proved that the human agreement was a necessary prerequisite to interagency interoperability and that, given the necessary political top cover and guidance, the technical teams from across the services, agencies and the Intelligence Community could work together to accomplish something meaningful.

From a technical perspective UCore was considered successful as a proof of concept. Although UCore V1.0 showed that the concepts of "when" and "where" could be defined in a universally understandable way and these two terms would be insufficient for meaningful information exchanges to support decision making or mission accomplishment. Finally UCore V1.0 showed that the XML community of practice is now mature enough to be able to implement machine-to-machine interoperability without any special tools or training. UCore V1.0 was submitted to the SESGG on October 04 2007 as the FY07 Working Group deliverable. The Working Group recommendation was to not mandate UCore V1.0 because of the perceived limitations and to immediately initiated UCore V2.0 development. However, several members of the user community did not agree that V1.0 was too small to be valuable and commenced immediate testing and implementation.

E. UCORE V1.0 PILOTS

Despite the working group recommendations the user community was poised to evaluate, test and implement Universal Core upon its release. Only a few actual implementations occurred but they were significant. It showed the Universal Core concept had some value to some operational end-users. The most illustrious example of end-user initiative is reflected in a Strategic Command (STRATCOM) project called SKIWEB.

As described by General Bob Kehler, Deputy Director of STRATCOM, SKIWEB stands for Strategic Knowledge Integration:

> …we use SKIWEB as a knowledge management network. We use it in the headquarters as a never-ending Ops Intel meeting, and in fact it is the key tool the senior leadership uses to stay abreast of events unfolding

> throughout the command and the world in real time… all prioritized by the commander's critical information requirements (Kehler, p.1).

Upon release of UCore the SKIWEB development team commenced refactoring the "where" and "when" concepts within their existing schema to UCore V1.0. The team had been working with various members of the, data community including Strike COI, Blue Force Tracking COI and Cursor on Target (COT). UCore V1.0 had borrowed from those initiatives, simplified and improved upon these two primary concepts. By November 2007, SKIWEB had imbedded UCore into their product and were testing it on their development LAN. The SKIWEB team initiated contact with the Ministries of Defense of United Kingdom and Australia and shared the concepts and schema with them. Over a period of a few short months, the SKIWEB team mandated that data producers create UCore compliant messages, was able to get National Security Agency Certification and Accreditation, and conducted successful experimentation with the Allies.

The value attributed to UCore V1.0 was that it forced data producers to conform to a standardized way of depicting time and location so that SKIWEB sources could be combined on a map without mediation. As of March 2008, SKIWEB had 12000 users, including the Chairman of the Joint Chiefs of Staff. This is an example of the flexibility of XML based technologies, the agility of Web 2.0 design teams, and the transformational power of motivated teams. The SKIWEB / UCore pilot is a shining example of the type of operationally driven capabilities promised by net-centric operations literature.

F. UCORE V2.0

Buoyed by the political success of the UCore V1.0 delivery in early October, DoD CIO and the IC CIO decided to invite the Department of Justice (DOJ) and the Department of Homeland Security (DHS) to contribute to the evolution of a common information specification that could be used across the four departments. DoD and the IC

had long standing and often mutually supportive relationships, but the addition of DHS and DOJ to the UCore V2.0 design and development team created significant political, technical and cultural challenges.

The most immediate and glaring of these challenges was that DOJ had already created and mandated a data model and framework called the National Information Exchange Model (NIEM) and had a concept of the universal cores and common cores embedded in that product offering. In addition, political tension existed between the developer communities because DoD and IC had evaluated NIEM and found it a valuable product, but one that was tailored to the Law Enforcement community and not generally applicable to the DoD / IC mission portfolios.

The first meeting of the UCore V2.0 development team occurred on 17 October 2007 less than two weeks after the release of V1.0. I was asked to continue to lead the effort and the Chief Technology Officer from the Department of Justice, Jeremy Warren, was assigned as the UCore V2.0 Development Working Group co-lead. My tasking from the Office of the Assistant Secretary of Defense was stated simply; "create something all the departments can agree on!" The government leads had confidence that a technical solution could be developed based on the lessons learned from UCore V1.0; however we were very aware that the political acceptance would be the driver behind UCore V2.0 adoption.

As fate would have it, the same week the UCore V2.0 kickoff meeting occurred, two important national policy documents were released, the President's "National Strategy for Information Sharing," and the "Cooperative Maritime Strategy for the 21st Century" co-signed by the Navy, Marine Corps and Coast Guard. Both these documents reflected the concepts of interagency information sharing in the context of missions that were common to all four departments. This provided a great opportunity for the government leads to jettison old baggage associated with previous efforts and focus on implementing these policies from a fresh perspective.

The challenges the design team faced for the development of UCore V2.0 were the same as during the UCore V1.0 remained. There was no dedicated funding, no

dedicated labor pool, and the schedule stretched to the end of the fiscal year. Since all the players had other responsibilities in their primary jobs, it was decided to design and develop as rapidly as possible before the UCore concept lost momentum. During the initial meeting, ground rules were set for participation, reporting responsibilities were established, success criteria were defined, and project termination conditions were articulated.

The DOJ and DHS representatives brought to the table a high level of political capital, experience with a mandated data model, and recent success with large scale data integration at the user community level. Most importantly however, the DOJ / DHS government team brought recent Web 2.0 technologies experience from commercial sector. In addition to the CTO, Justice also tasked their Chief Data Architect, Boris Shur, to support the effort. Boris, and the DHS lead, Anthony Hoang, had been members of the design and implementation team for Global Synchronization 1, and Boris was a data pool manager for the Global Data Synchronization Network (GSDN). GDSN standardized vocabularies for the retail industry to facilitate international commerce. Their website boasts that product sales of over 3 trillion dollars were executed over GDSN in 2007 (GDSN, 2008).

The DOJ lead, Mr. Warren, was also the National Information Exchange Model (NIEM) Program Manager who had accrued significant political capital by incorporating NIEM into the Counter Terrorism Information Sharing Standard (CTISS). The CTISS specification was a product of the Program Manager for the Information Sharing Environment, Ambassador Ted McNamara, Special Assistant to the President. DoD and the IC brought political capital, recent collaborative success on UCore V1.0 and various degrees of success from a number of data sharing initiatives. All four departments also brought the organizational baggage inherent in every large federal agency bureaucracy.

After several preliminary rounds of sparing, the government leadership and the volunteer support staff began to achieve traction on the Plan of Action and Milestones. It was agreed that regardless of the technical outcome, Universal Core V2.0 could be considered a success since it represented a level of interagency technical collaboration that had not been attempted before. With the fear of failure removed, the team spent six

weeks drafting a Vision and Scoping Document which describes the goals, schedules, definition of various levels of interoperability and articulated compliance profiles.

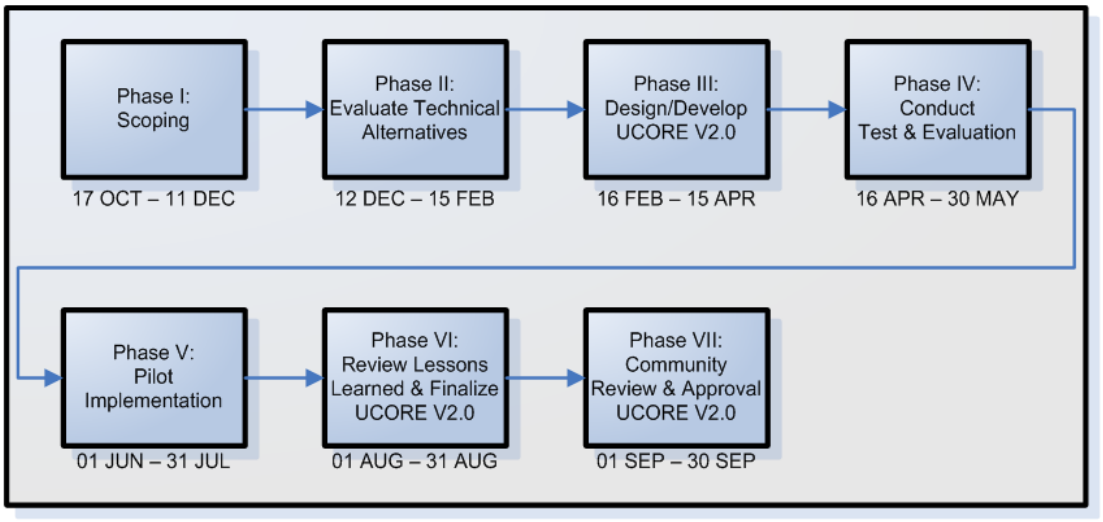


Figure 5-2: UCore V2.0 Plan of Action and Milestones

G. A CAPABILITIES DOCUMENT

The most important aspect of the Vision and Scope Document was that it permitted the individuals working on UCore V2.0 to congeal as a team and served as a de facto capabilities document for the effort. The document was drafted through continuous peer review in a period of less than six weeks and contained the assumptions, objectives, success criteria and schedule that served as the blueprint against which progress on the effort was measured.

The Vision and Scope Document describes a conceptual construct that is instantiated as an Information Exchange Specification and Implementation Profile. It is comprised of five parts (1) vocabulary and set of consistent data definitions for most commonly exchanged concepts (“who,” “what,” “where,” and “when”), (2) the XML representation of those concepts, (3) extension rules to allow tailoring to specific mission areas, (4) security markings to permit controlled access and electronic tear lines, (5) and a messaging framework to package and unpackage content consistently. The Vision and Scope Document was approved by the UCore ESC in early January.

The design phase of the effort began immediately thereafter with an abbreviated Analysis of Alternatives that evaluated the approaches to the "what, when, where, who" concepts from across the Federal Enterprise. Data models are architectural products that developers need to consistently implement information exchanges. In 1975 the American National Standards Institute (ANSI) described three levels of data schema; conceptual, logical and physical. Conceptual models describe the semantics of a domain and bound the scope of the model (Wikipedia, 2008).

Unfortunately the raw materials for the UCore preliminary analysis resulted in a compilation of 130 pages of Conceptual Data Models from various efforts. This proved impossible to review during the weekly teleconferences. Since all the models were essentially redundant and UCore quality metrics were based on simplicity, the Working Group leads tasked the design team to decompose the existing models and create one of no more than one page, on a Power Point slide. This was accomplished in a week. The development of this artifact, Figure 5.3 below, was the tipping point for UCore V2.0 design and permitted rapid progress and meaningful discussion by a distributed technical team of 40 engineers and subject matter experts who routinely dialed into the weekly meetings.

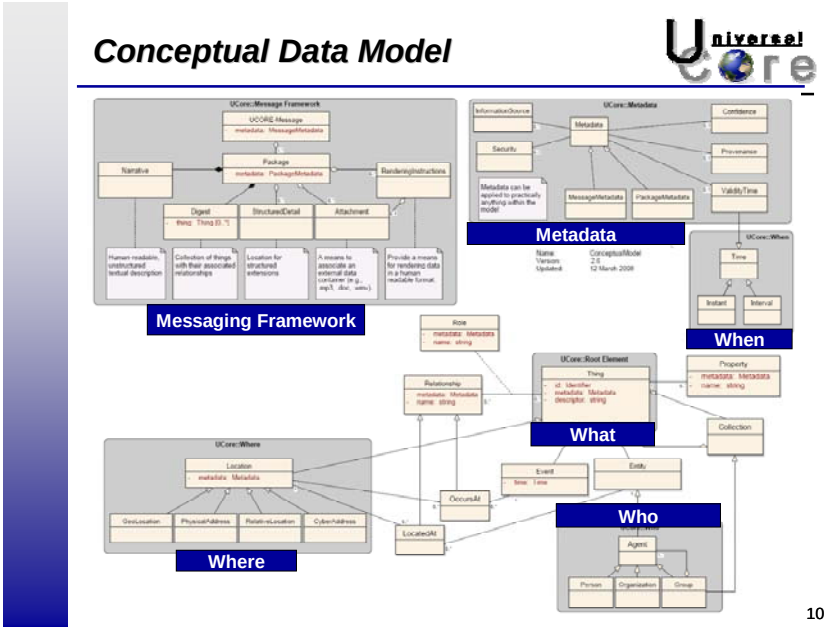


Figure 5-3: UCore V2.0 Conceptual Data Model

H. DESIGN / DEVELOPMENT PHASES

In order to remain on track the design team resorted to extreme programming methods. After the analysis period ended on 15 February, an eight week design and development period commenced. The team initiated one week spirals involving daily peer review, modification and updating. The end result was logical data models and physical instantiations of the concepts in XML Schema Descriptions (XSD). Additionally during this time the draft implementation guidance was developed. Peer review occurred in real time via teleconference and government review and approval occurred in near-real-time via email at the end of each business day. On April 16th, the government leads terminated the design phase and initiated two weeks of government review and documentation refinement. The UCore technical specification was released for interagency testing on 16 April which concluded 31 July 2008. Over 20 evaluation teams from DoD, DOJ, IC and DHS, all four military Services, DISA, two COCOMs, as well as the City of Colorado Springs are participated. A composite evaluation report is scheduled to be produced and released for community review on 15 August. Figure 5.4 below depicts the Developers Guide plus an example of the instance documents.

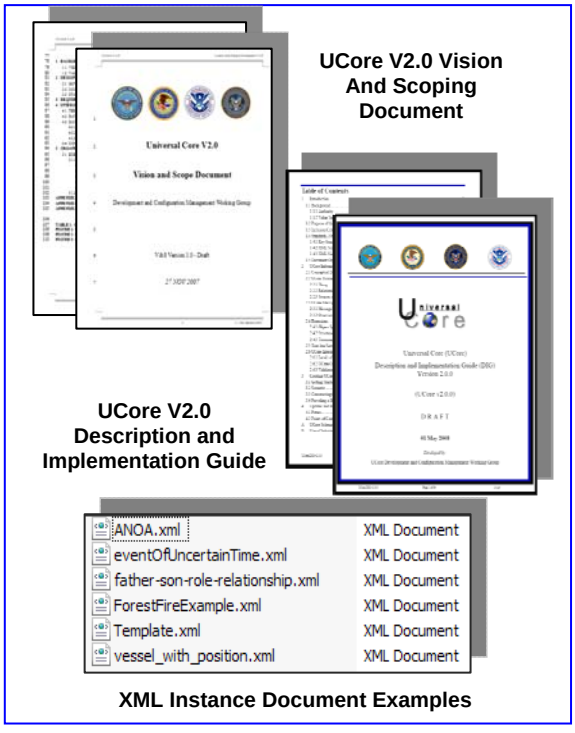


Figure 5-4: UCore V2.0 Artifacts

I. GOVERNANCE

The original governance structure of the Senior Enterprise Services Governance Group (SESGG) did not have DOJ and DHS representatives. Because there is no technical organization with authorities to span the Federal Government, a special Executive Steering Committee (ESC) was established to exercise UCore governance. The voting members are Deputy CIOs, from DoD, DOJ, DHS and the IC with advisory members from OMB (Chief Architect) and the Program Manager for Information Sharing Environment (PM ISE). This senior level participation made the UCore chain of command very short and decision making very efficient. Although not a formal acquisition effort, the ESC served in the capacity of a Milestone Decision Authority for the effort.

J. POLITICAL CAPITAL / TECHNICAL ADOPTION

The Universal Core effort has gained substantial political momentum over the past nine months. Momentum was fed by interagency design teams who either implemented or experimented with UCore V1.0 and by the growing number of UCore V2.0 Alpha testers who are reporting positive results from their preliminary findings. The government leads initially became concerned about the level of visibility and "pre-adoption" occurring across the communities. As noted in the following paragraphs, new policies, major programs of records, and a broad stakeholder base are all reflecting UCore as an emerging requirement for information sharing. After several weeks of attempting to evaluate risk, one government lead described the conditions as a "perfect storm," implying that political, technical and cultural conditions are converging during this effort (Peterson, 2000). Because it was no longer under their control, the team decided to acknowledge the risk and ride it out.

The UCore Executive Steering Committee has socialized UCore at the highest levels in the Federal Government. This has resulted UCore being an agenda items, topic of discussion or project of interest across a broad spectrum of stakeholders as noted in the bullets below:

- On 17 July, the Office of Assistant Secretary of Defense tasked the UCore Working Group leads to brief the Information Sharing Council, lead by the Special Assistant to the President and comprised of the Chief Information Officers (CIOs) of all Cabinet level departments. That briefing is scheduled to occur in September.
- On 15 July, the UCore government leads and the chief engineer, briefed the Interoperability Defense Science Board who will be incorporating the UCore lessons learned into their report to SECDEF Gates.
- UCore is being written into the rewrite of CJCS 6212.1E, "Interoperability and Supportability of Information Technology and National Security Systems "as part of the Net Ready Key Performance Parameter.
- UCore was briefed by the to ASD NII, John Grimes and the CIOs of all military services, JCS J6, the IC CIO and the DISA commander on 7 July. They have requested an update in September that includes the findings from the Alpha pilot teams.
- On 17 April 2008, the DoD CIO and IC CIO released a joint memorandum endorsing the UCore concept and encouraging its continued development.
- DHS and DOJ are currently drafting a joint UCore endorsement memo to be signed by the CIOs of the four principle departments that will encourage the use of UCore.
- The March 2008 Business Transformation Report to Congress cites on page 261, UCore as a "Key Program and Accomplishment" for Data and Services Implementation.
- PM ISE (Program Manager for Information Sharing Environment) incorporated UCore into the Counter Terrorism Information Sharing (CTISS) Specification and reflected the harmonization of UCore with the NIEM data model in the Information Sharing Environment Framework in March 2008.

K. SUMMARY

UCore can represent the human and technical starting point for improved interagency interoperability. It is based on the premise that a basic level of interoperability can be built into the Federal Enterprise by defining, standardizing and sharing a few fundamental information elements. This small, simple to implement vocabulary serves both as the technical cornerstone to build richer, more complex information exchanges and it can be used as an interface for legacy infrastructure integration. Stakeholders, technicians and managers can evaluate UCore in the context of their specific missions and lines of business. This reduces their individual risk but also creates a sense of ownership and participation in the process. Initial piloting efforts are reinforcing this assertion as will be described it the concluding chapter.

As a case study, UCore reflects the phases and challenges and potential success that apply to all Communities of Interest. The final chapter will highlight some preliminary results from the UCore Alpha testing teams are reporting and it will articulate how this thesis contributes to the literature on information sharing.

VI. THESIS CONTRIBUTION

The best way to achieve security is to prevent war.

Robert Gates, SECDEF
National Defense Strategy, June 2008

A. OVERVIEW

The new Maritime Strategy released in October 2007, articulates Navy tasking in the context of global security and highlights the roles maritime forces play in exercising political, economic and military forms of national power. The strategy stresses that the Navy must be prepared to win when forced to fight. However it places equal emphasis on enhancing deterrence capability, building national prestige and wielding economic might to stabilize an inherently volatile world. This same theme is reinforced in the National Defense Strategy released by the Secretary of Defense in June 2008. In it Secretary Gates states:

> We as a nation must strengthen not only our military capabilities, but also reinvigorate other important elements of national power, and develop the capability to integrate, tailor and apply these tools as needed.

This thesis has reviewed the tenets of Joint Vision 2020 and the technical concepts of DoD Transformation in the context of the new "Cooperative Maritime Strategy for the 21st Century." It hypothesizes that Decision Superiority requires a renewed emphasis on the fundamentals of decision making. The thesis asserts that in the emerging communications environment, information overload may be managed through greater discipline, e.g., Ignorance Management as a risk reduction concept to focus decision makers and supporting IT professionals on getting the "right information, to the right people, at the right time." This thesis introduces the concept of Information Readiness Levels to help operational forces more objectively gage the ability of the information architecture to support decision making in the context of specific missions. It also asserts that technical convergence has occurred and that the promise of network-centric operations can become a closer reality as organizational and cultural evolution

continues. The thesis contains examples of organizational evolution with a survey of portfolio management and Communities of Interest policies. Finally, the thesis concludes with a case study of the Universal Core, an interagency information sharing initiative that is an example of enterprise behavior and political, technical and cultural progress in this area.

B. FINDINGS

It appears that the tenets of earlier Navy and DoD net-centric doctrine remain valid. Information and Decision Superiority are force multipliers but the new Maritime Strategy entails viewing network-centric strategy from a different perspective. It places renewed emphasis on accelerating cultural change to use Network Centric Operations technologies to advance readiness in all mission areas. The need for viewing information requirements through a new lens is highlighted in "A Day in the Life of the Navy". The Chief of Naval Information press release states that on 14 May 2008 in addition to combat in the CENTCOM Theater of Operations, naval forces were engaged in "Operation Caring Response," "Operation Inspired Union," "Operation Continuing Promise" and "Pacific Partnership 08," a four month humanitarian deployment by the hospital ship USNS Mercy.

These new missions are being executed and superimposed upon an information sharing infrastructure tailored to support command and control, kill chains and battle damage assessment. A fair assessment is that the information architecture is groaning under the strain. U.S. Navy sailor inventiveness, and some progress in adopting a more agile Global Information Grid are showing promise, but are not enough. The Enterprise Information Environment is stretching, being redefined, and driving new data, information and decision support requirements. This thesis contributes to an understanding of how the IT, acquisition and data sharing communities are attempting to address these issues through an enterprise approach to data strategy implementation.

The concepts of right information, to the right person at the right time, are just as applicable to effective coordination in this new environment as they are in the timeless realm of warfighting. However, the Navy's emerging missions redefine somewhat the

concepts of "right," including calling for a reevaluation of information types, information partners and information qualities such as latency, trust and completeness. The requirements derived from new missions, and those that drive acquisition and data strategies, must reemphasize decision making as a process, rather than a solo event. Decision processes can be agile but they cannot be haphazard if decision superiority is to be achieved. Workflows, mission threads, and task sequences can support more consistent decision making, and when used in a SOA, can be made visible to the network and invoked as reusable services. When data qualities are defined in the context of the decision cycle, these services can be orchestrated and used to groom the information architecture to collect value-adding data, filter out noise and align the information products more closely with the business or mission needs.

Portfolio Management and Communities of Interest can represent political and organizational progress toward a net-centric environment. These constructs deal directly with the challenges of DoD functioning as an enterprise, not only from a joint operations perspective, but in the context of Planning, Programming, Budgeting, Execution and Acquisition. Communities of Interest are essentially Integrated Product Teams that are keyed to a data domain or information sharing problem. They provide support that DoD and Federal policies are being read, understood and executed. COIs are a manifestation of enterprise behavior. They are creating a vanguard of professionals who are gaining experience in the technical management challenges of large scale collaboration required for implementing a Services oriented architectural paradigm.

C. CASE STUDY RESULTS

The Universal Core was conceived as a way to improve interoperability between emerging Communities of Interest. It is founded on the premise that a basic level of interoperability can be built into the Federal Enterprise by defining, standardizing and sharing a few fundamental information elements. In a little over a year, it has evolved from concept paper into a multi-agency Federal, State and Local data-sharing initiative that has the potential to improve decision making, increase public confidence, and preserve taxpayer money. As a case study it reflects the real opportunities and limitations

of data sharing in a net-centric environment and is representative of the challenges that are faced by all Communities of Interest, agencies and departments.

The Universal Core, as a venue for interagency cooperation, is breaking down organizational barriers that have stymied meaningful technical exchanges between government executives and government engineers. Universal Core is being managed as an executive level Integrated Product Team (IPT) across four departments; IC, DoD, DOJ and DHS. The UCore team has analyzed new commercial standards, design patterns, architectural constructs and best practices from across the Federal Government to create a lightweight implementation profile that significantly reduces the technical and fiscal barriers to entry faced by organizations migrating to a net-centric environment. It also helps eliminate excuses for non-compliance to DoD and Federal policy.

UCore has the potential of saving the government significant development, integration, and sustainment costs. By providing a starting point for data model development and an interface for integration, dollars that would have previously been allocated to recreating these baseline elements can now be spent on improving the quality and precision of data being exchanged. The Universal Core also supports the concept of short term, highly specialized information exchanges for emerging missions. Institutional or ad hoc Communities of Interest can reuse the Universal Core and extend the baseline precepts to tailor their information architecture in an operationally feasible timeframe and at an acceptable cost. The Universal Core principle design criteria are simplicity and ease of use. Testing of initial versions of the specification indicate the concept is valid with pilot teams experiencing development times measured in terms of days and integration times in terms of weeks.

D. CASE STUDY IMPLICATIONS

On 23 July 2008, the UCore Working Group held its final meeting of the piloting phase. As usual this was done via teleconference. Everyone reported their status and the leads provided an update on the increasing level of visibility and political momentum the initiative was receiving. No discussion about Contract Line Item Numbers, cost overruns, or requests for additional schedule occurred. No contracts had been negotiated.

This group of professionals came together one last time, bound only by their desire to contribute to the effort. As the lead, I had to encourage and remind the teams to finish their reports, thank them for their contributions and wish them well in their future endeavors. It was a strange feeling to have managed a team that, with few exceptions, I recognized only through the sound of their voices or their email addresses.

In a practical sense, we had achieved interagency interoperability on the first day, when we had decided to consider ourselves a community of practice. The technical artifacts we created and tested merely allowed us to refine and sustain those roles. The team had arrived at consensus, captured and documented their agreements in the form of data assets and now desired to share their work with others. This has inspired the first UCore heuristic: All technical exchanges are predicated upon prior human agreement.

E. POLITICAL LESSONS LEARNED

In a less poetic vein, the implications and lessons learned from the case study can be grouped into three broad categories; Political, Technical and Cultural. Politically, the case study reinforces Step Two from the Community of Interest training slide introduced in Chapter 4, "Identify Champions, Members and Stakeholders." The primary lesson is that Step 2 is not a milestone but a continuous process. Data strategy implementation, when viewed as a data modeling exercise, can appear to be an esoteric art, practiced by intelligent, highly opinionated individuals from diverse technical and non-technical backgrounds. Champions and stakeholders can be end-users who neither understand nor care about the technical details. Stakeholder management is difficult, necessary and time consuming. Therefore, to maintain momentum, courting and gaining new champions can be the most powerful prime mover.

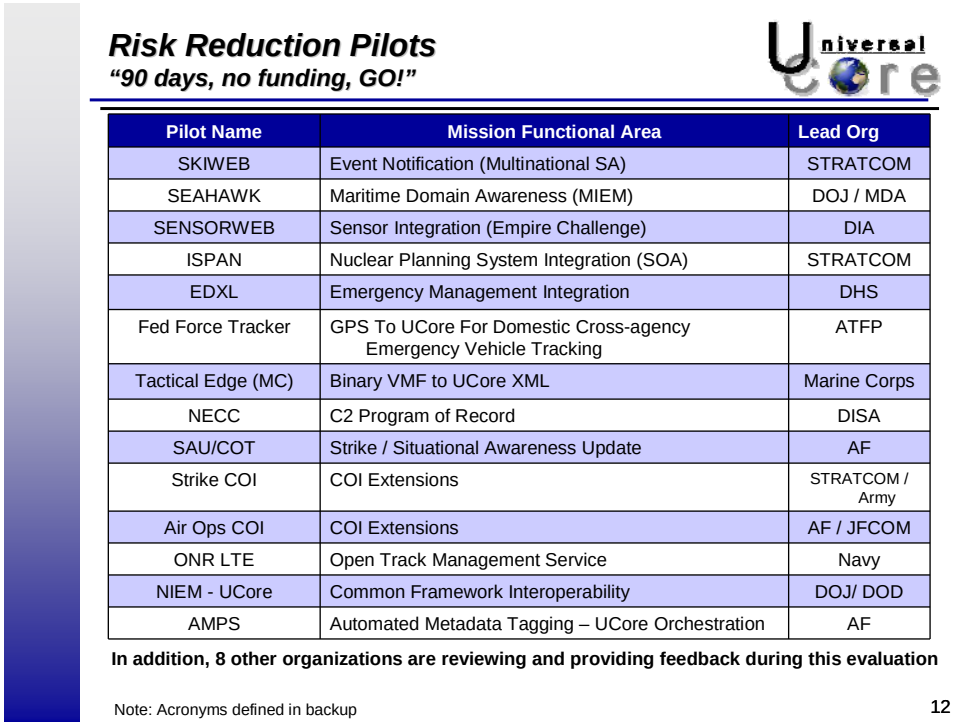
UCore was blessed with an energetic Senior Executive Service leader, Mr. Mike Krieger, who provided continuous support, encouragement and top cover to the government development team. Mr. Krieger brought the CIOs of the IC, DOJ and DHS to the table with the DoD CIO and worked tirelessly to keep them there. He briefed increasingly senior players about the potential of UCore and the progress the development team was making. These included the most senior uniformed officers in

DoD, political appointees and even a Special Assistant to the President. The UCore team also sought out organizational champions and used the fact that STRATCOM had incorporated UCore V1.0 into a tool being used by the Chairman of the Joint Chiefs of Staff as a low voltage prod to stimulate friendly competition between the organizations. This continuously growing number of champions inspired the technicians, permitted the government leads to create a "failure is not an option" culture, led to a great deal of peer review and ultimately resulted in a better product. These lessons confirmed the second UCore heuristic: "If you have no champions, you may be playing the wrong game."

An additional lesson learned from the use case is that in implementing the data strategy across the federal enterprise; there are no natural barriers. The bureaucracies that we have established to manage people and tasks are reinforced by our respective requirements, acquisition, and budgeting systems. These bureaucracies, however, do not represent the edges of the data domains for those organizations. Bureaucracies provide necessary stability and predictability but are frequent impediments to innovation. Enterprise behavior requires individuals to temporarily shed their organizational affiliations when they form data sharing communities and create a team culture. As an example of this, the government leads would rebuke each other for using the term "you" during meetings. Philosophically speaking, the collective capability of "we" was finite while the resources of "you" were perceived to be infinite. This business rule contributed to self-correcting behavior that resulted in more practical goals, processes and feasible deliverables. Heuristic number three is: In order to achieve interagency interoperability you must bend the bureaucracy to achieve the common good.

F. TECHNICAL LESSONS LEARNED

There were technical lessons learned from the UCore case study. The piloting teams are testing up to 50 function points associated with data formatting, extensibility and exchange. These lessons learned will be documented by the UCore Development Working Group and will be validated by a panel of senior government and industry personnel in mid-August. A slide from the UCore Executive brief lists the top 15 pilots.



Risk Reduction Pilots

"90 days, no funding, GO!"

Universal Core

Pilot Name	Mission Functional Area	Lead Org
SKIWEB	Event Notification (Multinational SA)	STRATCOM
SEAHAWK	Maritime Domain Awareness (MIEM)	DOJ / MDA
SENSORWEB	Sensor Integration (Empire Challenge)	DIA
ISPAN	Nuclear Planning System Integration (SOA)	STRATCOM
EDXL	Emergency Management Integration	DHS
Fed Force Tracker	GPS To UCore For Domestic Cross-agency Emergency Vehicle Tracking	ATFP
Tactical Edge (MC)	Binary VMF to UCore XML	Marine Corps
NECC	C2 Program of Record	DISA
SAU/COT	Strike / Situational Awareness Update	AF
Strike COI	COI Extensions	STRATCOM / Army
Air Ops COI	COI Extensions	AF / JFCOM
ONR LTE	Open Track Management Service	Navy
NIEM - UCore	Common Framework Interoperability	DOJ/ DOD
AMPS	Automated Metadata Tagging – UCore Orchestration	AF

In addition, 8 other organizations are reviewing and providing feedback during this evaluation

Note: Acronyms defined in backup

12

Figure 6-1: UCore V2.0 Risk Reduction Pilots (Source: UCore Executive Brief)

A few macro findings are already clear. Networking technologies, content sharing, syndication practices, maturation of technical standards, and the growth of a web-services community of practice have largely converged. The UCore initiative provides support that a ten year investment in net-centric concepts and eGovernment has created an environment conducive for advanced capability. UCore evolved from many other data sharing initiatives including Strike COI, Cursor on Target (CoT), and NIEM. The team was influenced by government leadership fresh from industry. It also tapped into a pool of existing talent funded for related efforts but dispersed on various projects.

Technical progress would have been more difficult if latent capability did not already exist. UCore development teams were merely provided a draft XML based specification and were asked to test and use the specification within the context of a mission area that they defined. They were offered no training or funding and were asked to work collaboratively to prove or disprove value of the specification in a period of 90 days. Twenty three teams volunteered because they were already working on data sharing efforts using XML based data exchange patterns, and they desired to orchestrate

or enhance their project with UCore. While none of the teams had any experience with the UCore V2.0 implementation profile, all of the team had experience with XML and the web-based services that permit XML content to be transferred over IP networks. Although there were costs associated with UCore, the teams bore them under their respective organization's execution year dollars, effectively distributing the fiscal burden of developing and testing Universal Core V2.0 across four Federal departments. The previous decade of investment allowed UCore to leverage the infrastructure and be developed and tested with no direct funding. In a very real sense, UCore constitutes the Return on Investment envisioned by net-centric theorists and stated in data sharing strategies. An example of this ROI is reflected in the orchestration of AMPS and UCore in what one developer enthusiastically described as "pure capability."

G. AMPS / UCORE

In late May 2008 the UCore leads provided a routine status update to the Service level Senior Enterprise Service Governance Group. The UCore update was followed by an Air Force representative who briefed the Automated Metadata Population Service (AMPS). Air Force had worked jointly with the other uniformed services on two versions of AMPS for approximately two years. Both concepts were endorsed by the SESGG. That afternoon the UCore team wrote the Air Force lead, Mr. Josh Powers, requesting additional information and expressing a desire for a technical exchange to occur. Mr. Powers responded and a technical exchange meeting (TEM) was scheduled for early May. The TEM was conducted via teleconference between three sites; San Diego, Colorado Springs and Washington DC. Having read the Power Point presentation concerning AMPS, UCore team wanted to know if their product could be used as part of AMPS to automatically tag unstructured data with the semantics from the UCore specification. Twenty minutes into the TEM, Mr. Powers indicated that if UCore could be place in an ontology format known as OWL, UCore could then serve as an annotator, or metadata template, for the unstructured data. At 25 minutes into the TEM, the UCore Chief Engineer, Brian Freeman, had converted the XML based schema into an OWL schema with a common commercial software tool. The technical exchange ended after

30 minutes with Mr. Powers indicating he had everything he needed. He told the government leads that he would report back after he tested the newly integrated components. At 2 PM that day, Mr. Powers sent a sample of the metadata tags that resulted from running 600 unstructured files through AMPS and indexing these files with UCore semantics. The total processing time was 20 minutes. In systems engineering terms this new "system" had evolved from concept exploration to design, development and proceeded through initial operational testing in less than one day. Total labor expended by both teams (e.g., three individuals) was approximately two hours. There was no software development and, with the exception of the conversion from XML to OWL, there was nothing that could be considered a modification of the two efforts.

The ability to automatically metadata tag structured and unstructured data is a watershed event. It contributes to solving one of the most challenging aspects of the net-centric data strategy; making data visible. This means that large volumes of useful data that the federal government collects, but which may not be visible enterprise-wide are now discoverable through common search engines. As importantly, this can be done in the context of the approved terms and definitions used by the federal government. Also because UCore is extensible and the AMPS annotator engine can accommodate these extensions, the possibility exists that data can be precisely tagged to specific mission areas and lines of business. This could reduce data overload, allow precision data indexing that could lead to significant improvements in providing the right information to the right person at the right time. The full implications of this effort are still under review and will be included in the final UCore evaluation report.

The ability to design a "service" that can ingest another design team's product to create a tailored, new capability is not special. In fact it is the state of the practice. Being Web 2.0 practitioners, Mr. Powers and Mr. Freeman did not even consider this an issue worthy of mention. The government leads however, were impressed. This concept of service orchestration, or choreography, is fundamental to Service Oriented Architectural paradigms and is in common use in industry. This rather long example resulted in heuristic number 5: With respect to the service oriented paradigm, the future is now.

H. CULTURAL LESSONS LEARNED

From a management perspective, probably the most interesting lessons learned from the case study relate to cultural change indicators, e.g., four Federal Departments started sharing their perspectives and requirements on interagency interoperability. Cultural change was also stimulated when diverse teams were allowed the freedom to develop rapidly and collaboratively in real-time. An organizational design feature was enhanced towards self-managing teams, resulting in a more productive and collaborative approach. While some were use to this type of extreme programming and rapid prototyping, others indicated they had never done it in a government project. Developers were not used to being allowed to execute a "try-fail-try again" design process under continuous government monitoring but without interference or the threat of negative repercussions. Government managers had modified or expanded their roles from customer to participant, as the developers were not under direct contract to the government leads.

Developers and modelers also had to reorient a traditional bureaucratic approach by learning to terminate development, often before they were comfortable with the product. The government leads had high thresholds for individual risk and decided to reduce it by sharing "work in process" with other development teams. This ultimately resulted in a massive peer review effort that reflected the influences of recent government experience in organizations and efforts like the Global Data Synchronization Network. To get an idea of the degree of peer review, the experienced government leads estimated the project would take a full-time team of five developers six weeks to complete. The initiative had no full time developers and no simple way to estimate the available labor hours. In the end, an estimated 80 engineers helped during the design and development phases. These two phases combined took 14 weeks. Because the peer review process brought in so many players, the government leads not only had a product at the end of the phase, but they had investments from a large number of organizations and a vested interest in success that facilitated the initiation and execution of the evaluation phase.

The government team also had to consciously change their perspective during the requirements development and the analysis of alternatives phases to ensure they were not focusing too exclusively on gaps and problems. The focus was on improving what already had proven successful rather than fixing what was wrong. This permitted the team to more accurately define what was feasible within the confines of the time and resource limitations. This focus on extending success rather than overcoming problems allowed the teams to make fast, visible progress and helped attract new champions, stakeholders and peer reviewers.

Another cultural indicator during the progress of the case was observing the emergence of a generational power shift. As the team lead during the briefing to the Defense Science Board on 15 July 2008, I stressed this point to the retired Service Secretaries, Flag and General Officers of the Board. My colleagues at the table constituted the UCore government leadership for the effort and one non-government engineer serving as Chief Engineer. All the government leads were GS-15 equivalents. Three of the six–team leads were under 32 years old. The Chief Engineer was 27. The other three government leads were over 50 years old. Only one of the government leads over 50 had any direct experience with Web 2.0 development. He was, however, acknowledged as brilliant and the "spiritual" leader of the technical team. This meant that although everyone was of equal "rank", the younger generation of players led and facilitated the project. This is mentioned as a positive cultural indicator, in that the acknowledgment of the technological competence of the younger participants facilitated and encouraged a successful outcome. Due to the speed at which technology is moving, an engineer under 40 is likely to be at the height of their technical capabilities, and capitalizing on this expertise connotes an evolving organizational maturity. Engineering expertise may or may not translate into equivocal managerial prowess, e.g., managing in a political arena.

The current popularity of the UCore concept will soon be tempered by the enormity of the tasks remaining. There is a great deal of effort, compromise and cost associated with achieving measurably improved government interoperability. However the current UCore buzz is representative of the kind of confidence that initial net-centric

successes can generate and build upon. The group of industry and government leaders that conducted the Web 2.0 exercise at Dartmouth is representative of this phenomenon:

> …[P]ractical leadership by senior executives will be called for to navigate through and derive business value from this transition to a more "open" form of engagement with both external constituencies and internal talent. While participants had varying views on the urgency of the transformation, a palpable spirit of optimism and excitement pervaded the group about the opportunities Web 2.0 presents to forward thinking companies in the coming years (Dartmouth, 2007).

This has inspired the final case study heuristic: In a Web 2.0 world, respect the grey-beard but start heeding the advice of no-beards.

I. AREAS FOR FUTURE RESEARCH

There are a number of topics within the net-centric data sharing area that are worthy of additional study. Following the outcome of the Universal Core Consolidated Evaluation Report for any technical, political or cultural implications of the Federal government's move to common data standards would be interesting. A review of the Portfolio Management construct would be valuable, possibly using the Warfare Mission Area and 8410.01 as a starting point to describe the challenges and successes of that new governance approach to information technology. A study that compares and contrasts successful and unsuccessful attempts at standing up Communities of Interest might prove useful. It could include the well established ones like Strike COI and emerging, or ad hoc COIs such as are being developed for the Africa Partnership Stations in the newly formed Africa Command. Evaluating and potentially maturing the concept of Information Readiness Levels would be a reasonable research topic especially for those newly arriving operational officers from the Fleet.

LIST OF REFERENCES

Albers, D. S., Garstka, J. J. & Stein, F. P. 1999. *Network Centric Warfare. Developing and Leveraging Information Superiority. Vienna, VA.: CCRP Publications Distribution Center.*

Allen, T. W., Conway, J. T., Roughead, G., 2007. *A Cooperative Strategy for 21st Century Seapower.* Retrieved 3 May 2008, from http://www.navy.mil/maritime/MaritimeStrategy.pdf.

Ayyub, Bilal M. 2003. *Risk Analysis in Engineering and Economics.* Chapman & Hall/CRC.

Barton, Linda G. 1997. *Quick Flip Questions for Critical Thinking*. Edupress, Inc.

Bly, Adam, (2008, January-February). The Too-Much Information Age. *Seed, 14, 59.*

Chairman of the Joint Chiefs of Staff . [CJCSa] 2008. [Unreleased Draft Revision], *CJCSI 6212.01E: Interoperability and Supportability of Information, Technology and National Security Systems.*

Chairman of the Joint Chiefs of Staff [CJCSb]. 2007. *CJCS Instruction 8410.01: Warfighting Mission Area Information Technology Portfolio Management And Net-Centric Data Sharing.*

Clark, Vernon, (August 2000) [OPNAV Staff brief upon assuming responsibilities as CNO]. Presented at Henderson Hall, Marine Corps Annex, Arlington VA.

Common Core Task Force, 2007. *Criteria for Universality and Utility of Information Structures.* Unpublished internal DoD report.

Dartmouth College, Tuck School of Business. 2007. *Web 2.0 and the Corporation: A Thought Leadership Roundtable on Digital Strategies.* Glassmeyer / McNamee School of Digital Strategies.

Department of Defense [DoDa], 1991. *DoD Directive 8320.1, DoD Data Administration.*

Department of Defense [DoDb], 2004. *DoD Directive 8320.02: Data Sharing in a Net-centric DoD.*

Department of Defense [DoDc], 2005. *DoD Directive 8115.01, Information Technology Portfolio Management*

Department of Defense [DoDd], 2006. *DoD Instruction 8115.02, Information Technology Portfolio Management Implementation.*

Department of Defense [DoDe], 2003. Net-Centric Operations and Warfare Reference Model.

Department of Defense [DoDf], 2007. DoD Architecture Framework, Version 1.5, Reference and Guidelines. Retrieved 2 August 2008, from http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_I.pdf.

Department of Defense MetaData Registry [MDR] (2008). [Based on access and review of the COIs listed on 27 June 2008] Retrieved 27 June 2008, from https://metadata.dod.mil/mdr/homepage.htm.

Frank, Sid. 2006. *Service Level Agreements for Data.* Published: June 6, 2006, Retrieved March 12, 2008, from http://www.b-eye-network.com/view/2956.

Gates, Robert. [Secretary of Defense]. 2008. *The National Defense Strategy*. Department of Defense.

Government Accountability Office [GAO], 2007. *Cost Assessment Guide: Best Practices for Estimating and Managing Program Costs.* GAO 07-1134SP.

Gladwell, Malcolm (2000). *The Tipping Point: How Little Things Can Make a Big Difference*. Boston: Little, Brown.

Global Synchronization 1, (2006). *The Global Data Synchronization Network*. Retrieved 1 February 2008, from http://www.gs1.org/productssolutions/gdsn/ds/what.html.

IEEE 90. Institute of Electrical and Electronics Engineers. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York, NY: 1990.

Kantner, James. (2001). *Knowledge Centric Organization (KCO) Assessment*. Department of the Navy Chief Information Officer.

Kehler, Robert. 2006. [Speech] Lieutenant General Bob Kehler, Deputy Commander, U.S. Strategic Command AFCEA Convention Washington, D.C. 16 June 2006. Retrieved 15 May, 2008, from htttp://www.stratcom.mil/Spch&test/CD_AFCEA_16Jun06.html.

Loshin, David (2007). [Brief] *A Process For Data Requirements Management*. Knowledge Integrity. Inc. E-mail correspondence, 15 December 2007.

Maier M., W., Rechtin, E., 2000. The Art of Systems Architecting. CRC Press.

MITRE, 2006. Study of Message Traffic. Unpublished paper.

National Security Council [NSC], 2007. National Strategy for Information Sharing. Retrieved 28 November 2008, from http://www.whitehouse.gov/nsc/infosharing/index.html

Nordhaus, William D. *The Story Of A Bubble. The New York Review Of Books*. Volume 51, Number 1 · January 15, 2004. Retrieved 2 August 2008, from http://www.nybooks.com/articles/16878

Patterson, E. S., Roth, E. M., Woods D. D., (1999). *Aiding the Intelligence Analyst in Situations of Data Overload: a Diagnosis of Data Overload.* Institute for Ergonomics/Cognitive Systems Engineering Laboratory Report (1998) ERGO CSEL 9902.

Peterson, Wolfgang. (Director) (2000). *Perfect Storm*. [WithGeorge Clooney, Mark Wahlberg, Mary Elizabeth Mastrantonio]. United States. Warner Brothers.

Powell, Colin (2008) [Brief] *A Leadership Primer*. Retrieved 4 April 2008 from http://govleaders.org/powell.htm

Powner, David A. (2008). *OMB and Agencies Need to Improve Planning, Management, and Oversight of Projects Totaling Billions of Dollars. Government Accountability Office*. Government Accountability Office, GAO-08-1051T

Rigalski Shari, 2007 [Chart] *CIOs Value a Full Information Management Strategy*, DM Review Magazine, September 2007 Volume 17, Number 9.

Roughead, Gary. [Chief of Naval Operations]. 2007. *Operating at the Convergence of SeaPower and Cyberpower*. Strategic Studies Group XXV II Charter (SSG XXVII)

Roughhead, Gary. [Chief of Naval Operations] 2007. *Rhumblines: 06 December 2007*. Chief of Naval Information internal Navy release.

Secretary of the Navy, [SECNAV]. 2005. SECNAV Instruction 5000.36A: *Department Of The Navy Information Technology Applications And Data Management.* Office of the Chief Information Officer.

Shalikashvili, John 1995. *Joint Vision 2010*. Department of Defense. Retrieved 14 February 2008, from http://www.dtic.mil/jv2010/jv2010.pdf.

Shelton, Henry, H., 2000, *Joint Vision 2020*. Office of Primary Responsibility: Director for Strategic Plans and Policy, J5; Strategy Division Published by: U.S. Government Printing Office, Washington DC, p.11. Retrieved 14 February 2008, from http://www.dtic.mil/jv2020/jv2020.pdf

Stenbit, John, P. 2003. *DoD Net-centric Data Strategy*. Department of Defense Chief Information Officer (CIO).

Toffler, Alvin, [Quote attributed to Mr. Toffler]. Retrieved 7 July 2008, from http://www.stanfordalumni.org/news/magazine/2002/janfeb/upfront/presidents.html

U.S. Joint Forces Command, 2004. *Joint Transformation Roadmap*, Submitted by U.S. Joint Forces Command to Director, Office of Force Transformation

Wennegren, David, (2007, July). *Interview with David M. Wennergren, Deputy Assistant Secretary of Defense (Information Management and Technology), DoD Deputy Chief Information Officer*. Retrieved 2 August 2008, from http://www.military-information-technology.com/article.cfm?DocID=2079

Wikipedia, 2008. Various definitions downloaded from Wikipedia throughout the research period from http://www.wikipedia.org/

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. RADM Michael Bachmann
   Space and Naval Warfare Systems Command
   San Diego, CA

4. RDML Jerry Burroughs
   Space and Naval Warfare Systems Command
   San Diego, CA

5. Mr. Carl Siel
   Office of the Assistant Secretary of the Navy, Research, Development and Acquisition
   Washington, DC

6. Ms. Michelle Bailey
   Space and Naval Warfare Systems Command
   San Diego, CA

7. Dr. Bill Rix
   Space and Naval Warfare Systems Command
   San Diego, CA

8. Dr. Paul. Sheblin
   Meyer Institute
   Naval Postgraduate School
   Monterey, CA